Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студентки ***Удовик Марії Олексіївни***

академічної групи *125-18-1*

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему ***Комплексна система захисту іформації іформаційно-телекомушкаційної системи ТОВ «Українські Інноваційні Технології»***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н.проф., Корнієнко В.І.			
розділів:				
спеціальний	ст.викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.	*90*	*відмінно*	
Рецензент				
Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
Завідувач кафедри
безпеки інформації та телекомунікацій
_____д.т.н., проф Корнієнко В.І.
«___»_____2022 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Удовик Марії Олексіївні*** **академічної групи** ***125-18-1***
(прізвище та ініціали) (шифр)
спеціальності ***125 Кібербезпека***
спеціаліації[1] _____
за освітньо-професійною програмою ***Кібербезпека***

на тему ***Комплексна система захисту іформації іформаційно-телекомушкаційної системи ТОВ «Українські Інноваційні Технології»***

Затверджую наказом ректора НТУ «Дніпровська Політехніка» від 268-с 18.05.2022

Розділ	Зміст	Термін виконання
Розділ І	*Обстеження інформаційно-телекомунікаційної системи ТОВ «Українські Інноваційні Технології», розробка моделі порушника аналіз актуальних загроз.*	25.04.2022-04.05.2022
Розділ 2	*Визначення послуг безпеки, аналіз існуючого стану послуг безпеки в ІТС, розробка проектних рішень*	05.05.2022-21.05.2022
Розділ 3	*Економічне обґрунтування доцільності впровадження запропонованих рішень кваліфікаційної роботи*	21.05.2022-08.06.2022

Завдання видано: _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 08.01.2022р.

Дата подання до екзаменаційної комісії: 10.06.2022р.

Прийнято до виконання _____ Удовик М.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 95 с., 10 рис., 20 табл., 4 додатка, 8 джерел.

Об’єкт розробки: система захисту інформації в ІТС підприємства ТОВ «Українські Інноваційні Технології»

Метою кваліфікаційної роботи є захист інформації що обробляється в інформаційно-телекомунікаційній системі на заданому рівні.

У першому розділі було виконано обстеження ІТС, а саме :

- фізичного середовища;
- обчислювальної системи;
- середовища користувачів;
- оброблювана інформація і технології її обробки;
- модель порушника, актуальні загрози для інформації, що циркулює в ІТС.

У другому розділі було сформульовано вимоги до послуг безпеки інформації у вигляді профілю захищеності. На основі якого запропоновані проектні рішення, що реалізують послуги, які були відсутні.

У економічному розділі було визначено доцільність впровадження КЗЗ та технічних заходів, розраховано капітальні, експлуатаційні витрати, річний економічний ефект, показник економічної ефективності розробки та впровадження КЗЗ.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ПОРУШНИКА, МОДЕЛЬ ЗАГРОЗ, ПРОФІЛЬ ЗАХИЩЕНОСТІ.

ABSTRACT

Explanatory note: 95 pages, 10 pictures, 20 tables, 4 appendices, 8 sources.

Object of development: information protection system of the enterprise LLC "Ukrainian Innovative Technologies"

The purpose of the qualification work is to protect the information processed in the information and telecommunications system at a given level.

In the first section, an ITS survey was performed, namely:

- physical environment;
- computer system;
- among users;
- processed information and technologies of its processing.

intruder model, current threats to information circulating in the ITS

In another section, the requirements for information security services were formulated in the form of a security profile. On the basis of which the project decisions realizing services which were absent are offered.

The economic section determined the feasibility of developing new and improving existing means of information protection, calculated capital, operating costs, annual economic effect, economic indicator.

INFORMATION SECURITY, RESTRICTED INFORMATION, COMPREHENSIVE INFORMATION PROTECTION SYSTEMS, VIOLATION MODEL, THREAT MODEL, PROTECTION PROFILE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСТУ – державний стандарт України;

ЕОТ – електронно-обчислювальна техніка;

ІзОД – інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КС – комп'ютерна система;

НД – нормативний документ;

НСД – не санкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПЕМВН – побічне електро-магнітне випромінювання;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

ПКП – приймально-контролюючий пристрій;

ТЗІ – технічний захист інформації.

ЗЕД – зовнішньоєекономічна діяльність

ТЗ – технічне завдання

ЗМІСТ

С.

ВСТУП

Україна знаходиться на етапі поновлення стандартів ІБ та покращення процесів і функцій стосовно створення умов безпечного існування інформаційного середовища. Держава досягає вирішення даних питань завдяки аналізу сусідніх країн, які мають більший досвід в контексті реакції на певні інформаційні проблеми та методів їх знешкодження. Одним із джерел здобування досвіду стосовно безпеки інформації та її середовища можна вважати підприємства комерційного характеру, які знаходяться на території самої держави.

У даній роботі буде розглянуто задачу про встановлення КСЗІ і її реалізації за допомогою КЗЗ та методів вирішення даної задачі в аспекті затвердження КСЗІ для підприємства, також буде зроблено висновки стосовно впровадження КСЗІ на даному підприємстві, виходячи із інформаційних витоків, загроз та інших негативних факторів, які можуть підривати авторитет та економічний стан описаного нижче підприємства. У першому розділі буде описано загальні риси підприємства, а саме:

- Загальний опис підприємства (вид діяльності, галузі розробки продуктів тощо);
- загальна інформація;
- обстеження ІТС підприємства;
- аналізування моделі загроз, вразливостей та моделі порушника;
- існуючі механізми захисту ІТС підприємства та їх огляд. (політики, стандарти стосовно забезпечення ІБ підприємства тощо)

Вся описана інформація у даній роботі може бути зміненою у зв'язку із політикою конфіденційності організації, але на достовірність даної роботи змінена інформація не впливає.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ.

1.1 Загальні відомості.

Об’єктом інформаційної діяльності є підприємство «Українські Інноваційні Технології».

Компанія ТОВ «Українські Інноваційні Технології» займається розробкою та експлуатацією додатків, сайтів для різних галузей, таких як:

- освіта;
- медицина;
- авіація;
- транспортні послуги.

Компанія почала вести свою діяльність із 2015 року. За 7 років введення власної діяльності, підприємство розробило приблизно 15 різних видів продуктів різнопланового характеру.

На даний період часу ТОВ «Українські Інноваційні Технології» розробляє мобільне ПЗ, головна ціль якого - забезпечення пошуку транспорту в будь-якому місті України для подальшої його оренди.

Організаційна структура управління компанією зображена на рис. 1.1.

Компанія працює з 9.00 до 18.00.

Постійний штат співробітників складає 17 осіб:

- 2 бізнес-аналітика;
- 5 розробників;
- 5 тестувальників;
- 1 генеральний директор;
- 1 старший системний адміністратор
- 1 системний адміністратор;
- 1 бухгалтер;
- 1 охоронець.

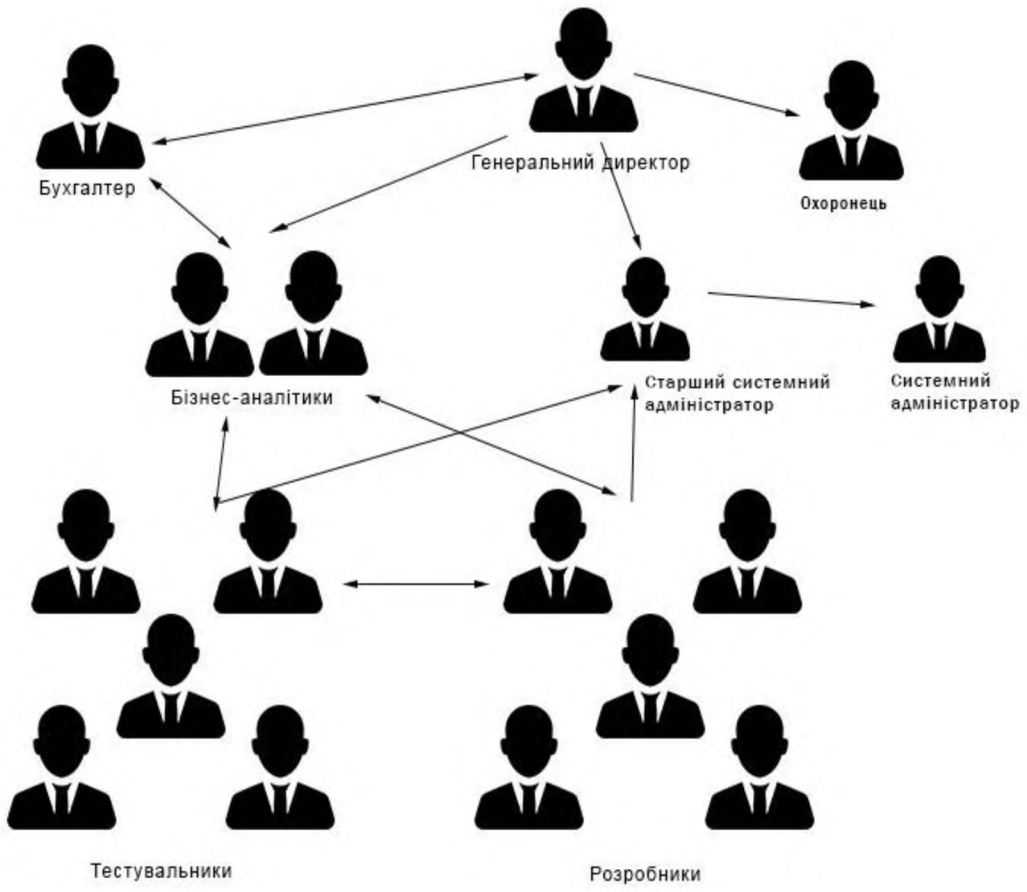

Рисунок. 1.1 - Організаційна структура управління компанією

1.2 Обґрунтування необхідності створення КСЗІ в ІТС

Згідно ЗУ «Про інформацію» статті 20 пункту 1:

1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Згідно ЗУ «Про інформацію» статті 21 Інформація з обмеженим доступом:

1. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

2. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Згідно ЗУ «Про захист персональних даних» статті 5 пункту 1 об’єктами захисту є персональні дані.

Згідно ЗУ «Про захист персональних даних» статті 10 пункту 2,

використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних. Володільцю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними.

Згідно ЗУ «Про захист інформації в ІТС» статті 5: власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі.

Згідно Цивільного Кодексу України статті 505:

1. Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

2. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Згідно статті 506 Цивільного Кодексу України, майнові права інтелектуальної власності на комерційну таємницю визначається наступними правами за пунктами:

1. Майновими правами інтелектуальної власності на комерційну таємницю є:

1) право на використання комерційної таємниці;

2) виключне право дозволяти використання комерційної таємниці;

3) виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці;

4) інші майнові права інтелектуальної власності, встановлені законом.

2. Майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визначила інформацію комерційною таємницею, якщо інше не встановлено договором.

Згідно Цивільного Кодексу України статті 433:

1. Об'єктами авторського права є твори, а саме:

1) комп'ютерні програми;

2) компіляції даних (бази даних), якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності;

4. Комп'ютерні програми охороняються як літературні твори.

5. Компіляції даних (бази даних) або іншого матеріалу охороняються як такі. Ця охорона не поширюється на дані або матеріал як такі та не зачіпає авторське право на дані або матеріал, що є складовими компіляції.

Згідно закону України «Про захист інформації в інформаційно-комунікаційних системах» статті 9 про забезпечення захисту інформації в системі:

- відповідальність за забезпечення захисту інформації в системі покладається на власника системи;
- власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним;

Так як в ІТС ТОВ «Українські Інноваційні Технології» комерційна таємниця, персональні дані а саме інтелектуальна власність - обробляється ІзОД, а саме, їх необхідно захистити згідно закону України «Про інформацію» та «Про захист інформації в інформаційно-комунікаційних системах».

Щоб захистити інформацію необхідно побудувати КСЗІ для виконання вимог захисту інформації.

Для обґрунтування вимог до режимних заходів було проведено категоріювання ОІД:

Категоріювання проводилось згідно НД ТЗІ 1.6-005-2013 було проведено категоріювання приміщення, на якому здійснюється обробка технічними засобами ІзОД, що не становить державної таємниці. ОІД відноситься до 4 категорії. Акт категоріювання наведено в додатку А.

Порядок проведення робіт і комплексу взаємоузгоджених заходів із впровадження КСЗІ в ІТС визначено у НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

Згідно НД ТЗІ 3.7-003 -2005 необхідно провести обстеження середовищ функціонування ІТС, а саме таких її складових:

- фізичного середовища;
- обчислювальної системи;
- інформаційного середовища;
- середовища користувачів.

На основі результатів обстеження потрібно:

- розробити модель загроз;
- виконати аналіз актуальних загроз;
- розробити політику безпеки;
- запропонувати проектні рішення щодо реалізації послуг безпеки.

Створення і впровадження КСЗІ значно знизить економічні втрати підприємства від реалізації потенційних загроз, які будуть визначені на етапі аналізу моделі загроз та моделі порушника.

1.3 Обстеження середовищ функціонування ІТС

ОІД знаходиться в будівлі за адресою: Україна, м. Дніпро, вул. Короленко, 4. Будівля, в якій знаходиться ОІД, що обстежується, має чотири поверхи, знаходиться на другому поверсі. ОІД складається з 5 кімнат: директора, серверної, кабінету тестувальників, бізнес-аналітиків, розробників. Також є коридор.

1.3.1 Обстеження фізичного середовища

Ситуаційний план приведено на рис. 1.2.

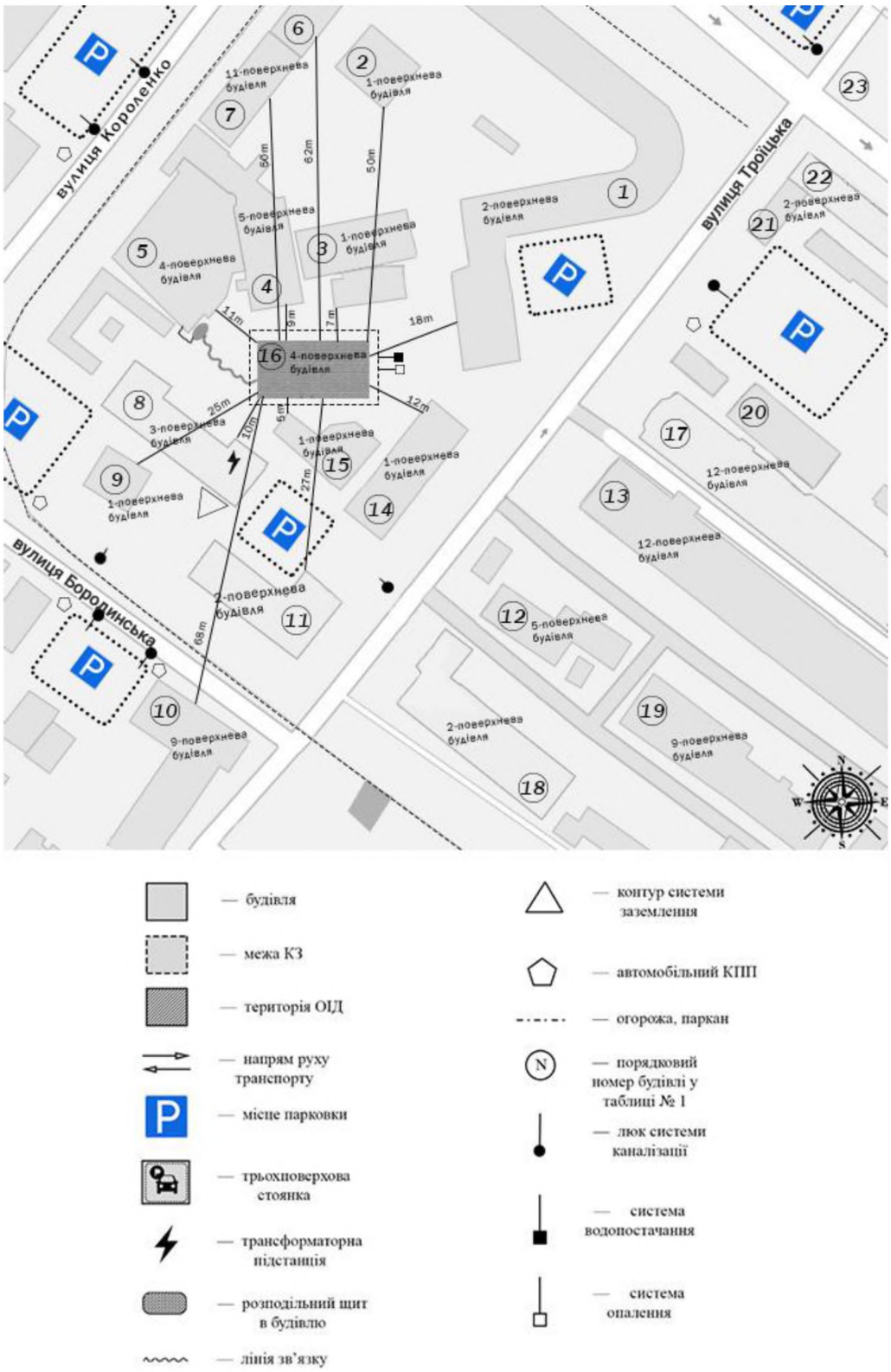

Рисунок 1.2 - Ситуаційний план

Будівля, в якій знаходиться ІТС, що обстежується, має чотири поверхи і збудована з керамічної цегли. Дах будівлі виконаний з металочерепиці, який є стійким до вогню і має клас А по вогнестійкості. Не горить, не підтримує горіння.

Навколо будівлі, де знаходиться ОІД, розміщені такі об'єкти:

- на півночі знаходяться чотири будівлі, 1-поверхова, 5-поверхова, 11-поверхова(житлова) та 1-поверхова будівлі, також вулиця Короленко,
- на півдні знаходиться дві 1- та 2-поверхові адміністративні будівлі,
- на заході знаходиться одноповерховий господарський корпус та 3-поверхова адміністративна будівля та вулиця Бородінська,
- на сході знаходиться одноповерховий господарський корпус та 2-поверховий адміністративні будівлі, та вулиця Троїцька.

Опис вулиць:

- на північно-східній стороні односмугова вулиця вулиця Троїцька;
- на північно-західній стороні односмугова вулиця Короленко;
- на південній стороні односмугова вулиця Бородінська;

Увесь детальніший список будівель та споруд в табл. 1.1.

Таблиця 1.1 - Характеристика будівель та споруд

№	Найменування	Кількість поверхів	Адреса	Відстань до ОІД, м
1	Адміністративна будівля	2	Вул. Троїцька, 10	18
2	Адміністративна будівля	1	Вул. Короленко, 12	50
3	Адміністративна будівля	1	Вул. Короленко, 12а	7
4	Адміністративна будівля	5	Вул. Короленко, 12	9
5	Господарський корпус	4	Вул. Короленко, 18	10
6	Житлова споруда	11	Вул. Короленко, 20	62
7	Житлова споруда	11	Вул. Короленко, 20а	50

№	Найменування	Кількість поверхів	Адреса	Відстань до ОІД, м
8	Господарський корпус	3	Вул. Короленко, 22	10
9	Господарський корпус	1	Вул. Короленко, 30	25

Продовження таблиці 1.1

10	Житлова споруда	2	Вул. Короленко, 4а	68
11	Адміністративна будівля	2	Вул. Короленко, 4д	27
12	Житлова споруда	1	Вул. Короленко, 4б	48
13	Житлова споруда	1	Вул. Короленко, 6	50
14	Господарський корпус	1	Вул. Короленко, 8г	7
15	Адміністративна будівля	1	Вул. Короленко, 11	5
17	Житлова споруда	12	Вул. Короленко, 13	55
18	Житлова споруда	2	Вул. Короленко, 19	50
19	Житлова споруда	9	Вул. Короленко, 15	87
20	Житлова споруда	3	Вул. Бородінська, 18	70
21	Житлова споруда	2	Вул. Троїцька, 11	76

Опис тих систем, що підключені до будинку:

Лінії систем водопостачання, мають вихід за межі КЗ, підключені до міської системи водопостачання.

За межі ОІД, виходить лінії систем водопостачання, опалення, електроживлення, освітлення та Інтернету.

Лінії систем електроживлення йдуть у щитову будинку. З електричного щитка лінії освітлення та електроживлення йдуть до трансформаторної підстанції, що показано на рис. 1.2. У результаті роботи ОІД часто виникає перенавантаження мережі електропостачання.

ОІД, що обстежується, знаходиться на другому поверсі:

- стіни ОІД зроблені з керамічної цегли, товщина стін 0,3 м.;

- підлога та стеля мають бетонні конструкції близько 0,15 м.;
- підвісна стеля зроблена з металу та пластику;
- ОІД має один вхід\вихід, на якому встановлені захисні вхідні металеві двері шириною 1 м. та товщиною 0,08 м.
- В ОІД сім ламінованих міжкімнатних дверей з основою дерев'яної конструкції, порожнечі якої заповнені пінополіуретаном для збільшення міцності і звукоізоляції. Кожні двері мають циліндровий штифтовий замок із захисною накладкою. Такий замок має середній рівень якості захисту та мають не надто високу стійкість до злому - розкривається відмичками, найчастіше розкривається шляхом виламування циліндра ломом, розкривається зі значним шумом до 15 хв. Кожен робітник має два ключі: від вхідних дверей та дверей свого відділу. Директор має доступ до кожної двері, в нього є ключі від кожного приміщення. Міжкімнатні двері кожного відділу мають ширину 0,8 м. та товщину 0,03 м.;
- В приміщені чотири віконних отвори, товщина вікна 0,02 м., складаються с склопакету та пластику. Також на кожному вікні є внутрішні металеві грати. На ОІД з східної та західної сторони встановлено віконні отвори.

Схема генерального плану представлена на рис. 1.3.

На ОІД є такі технічні системи: електропостачання, освітлення та комп'ютерної мережі (представлено на рис. 1.4), опалення та водопостачання (представлено на рис. 1.5), вентиляції та кондиціювання (представлено на рис. 1.6), охоронної та пожежної сигналізації (представлено на рис. 1.7).

Розетки системи електропостачання мають паралельне з'єднання та підключається до електричної щитової офісу, що в свою чергу підключена до щитової що знаходиться на першому поверсі з міжповерховим переходом.

За межі ОІД, виходить лінії систем водопостачання, опалення, електроживлення, освітлення та Інтернету.

Лінії освітлення та електроживлення йдуть у електрична щитова офісу. З електричного щитка лінії освітлення та електроживлення йдуть в трансформаторну підстанцію, що показано на рис. 1.2. У результаті роботи ОІД часто виникає перенавантаження мережі електропостачання.

Підприємство використовує централізоване опалення, тому лінії опалення виходить за межі ОІД та направляється на південь до вулиці Короленко.

На ОІД використовуються ноутбуки, маршрутизатор, комутатор, сервер, принтера, повний список ресурсів приведений в табл. А.1 Перелік апаратного забезпечення ІТС, структурна схема якої представлена на рис. 1.8. Використовуються системи пожежної та охоронної сигналізації, список приведений в табл. А.2 інвентаризаційна відомість ДТЗС. Повна характеристика складу ІТС приведена в табл. А.3. На ОІД використовуються системні, прикладні та спеціальні програмні забезпечення, детальний опис в табл. А.4. Інвентаризаційна відомість програмного забезпечення ІТС.

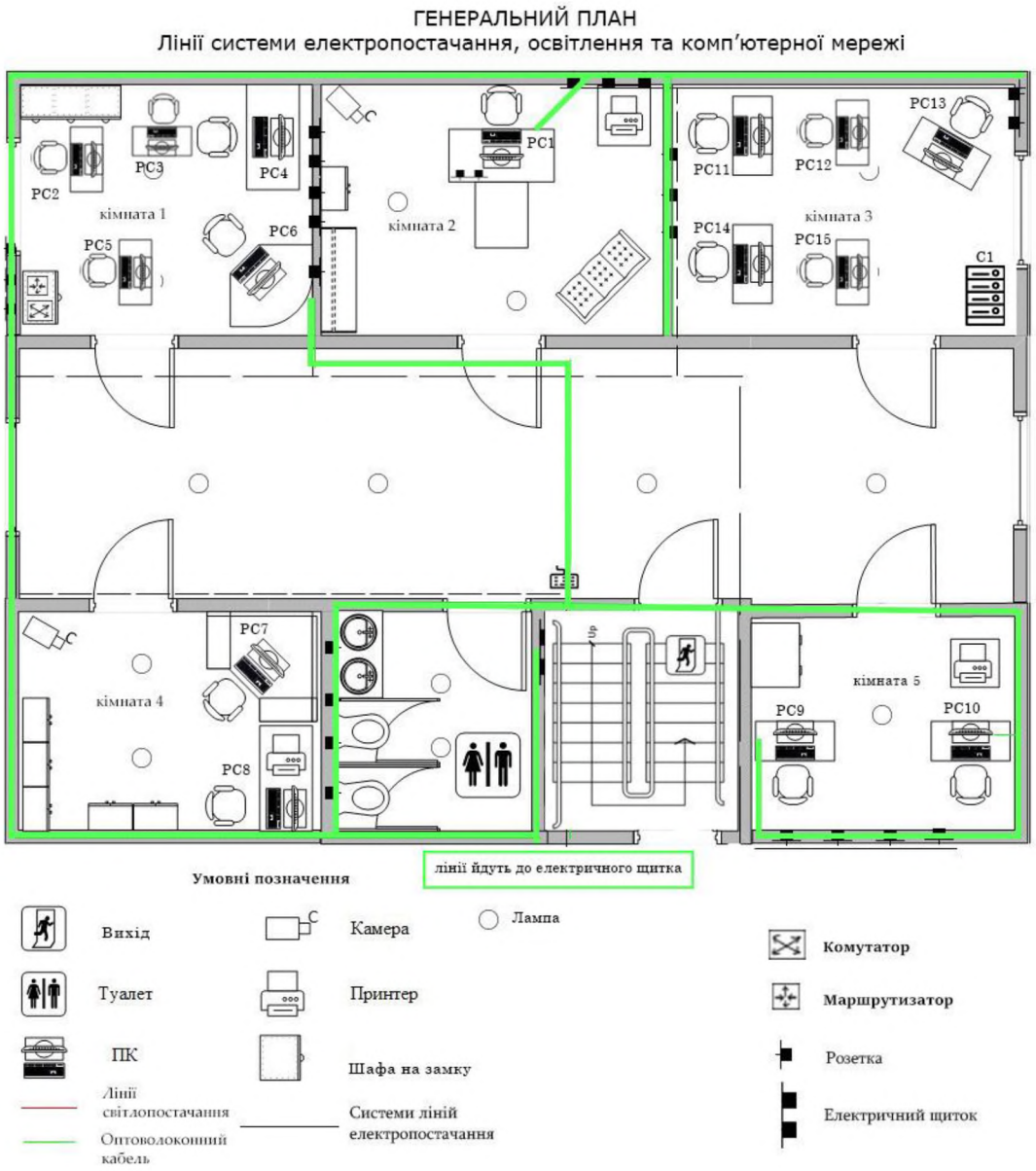

Рисунок 1.4. - Генеральний план. Лінії системи електропостачання, освітлення та комп'ютерної мережі

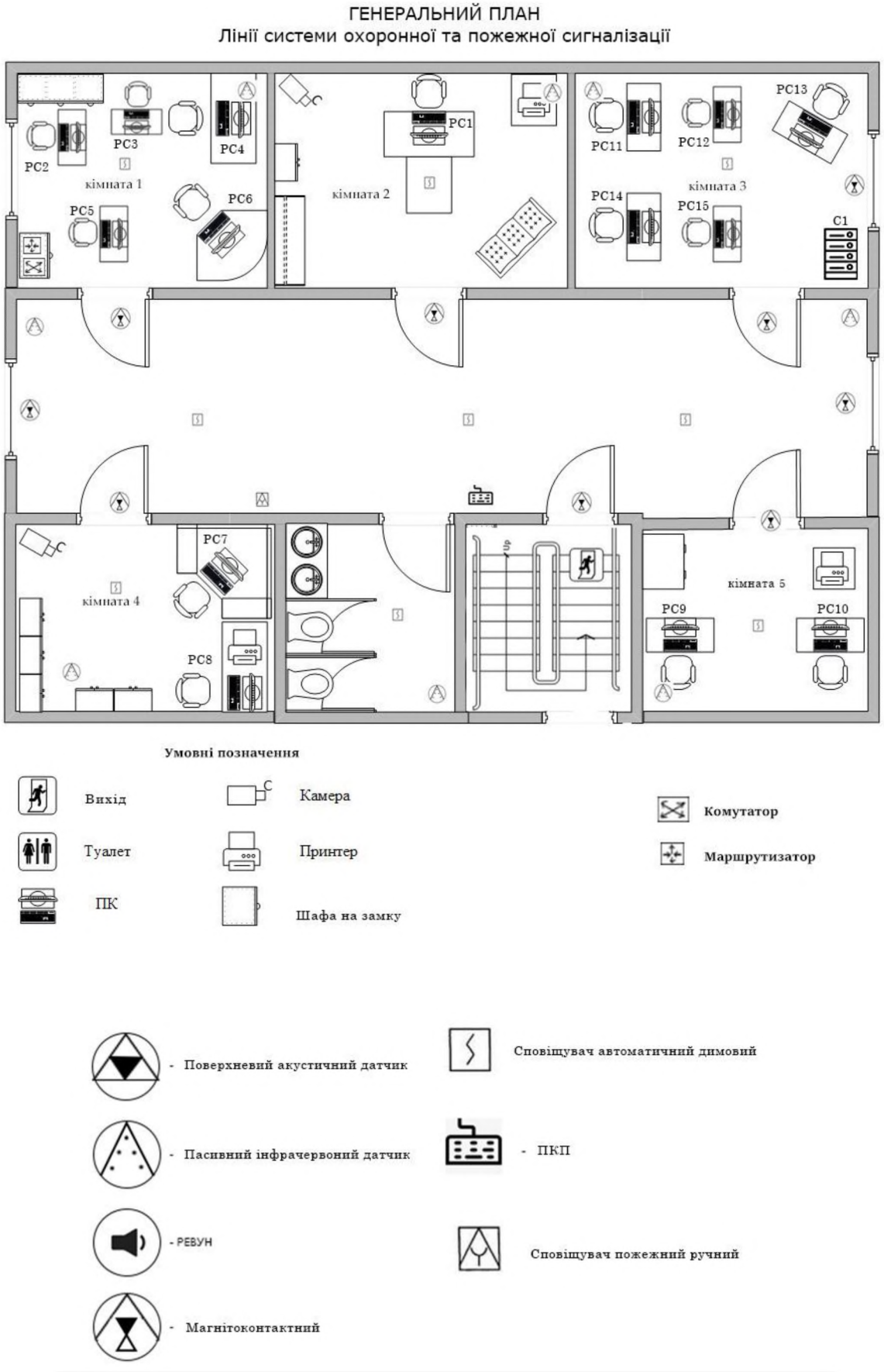

Рисунок 1.3. - Генеральний план ОІД

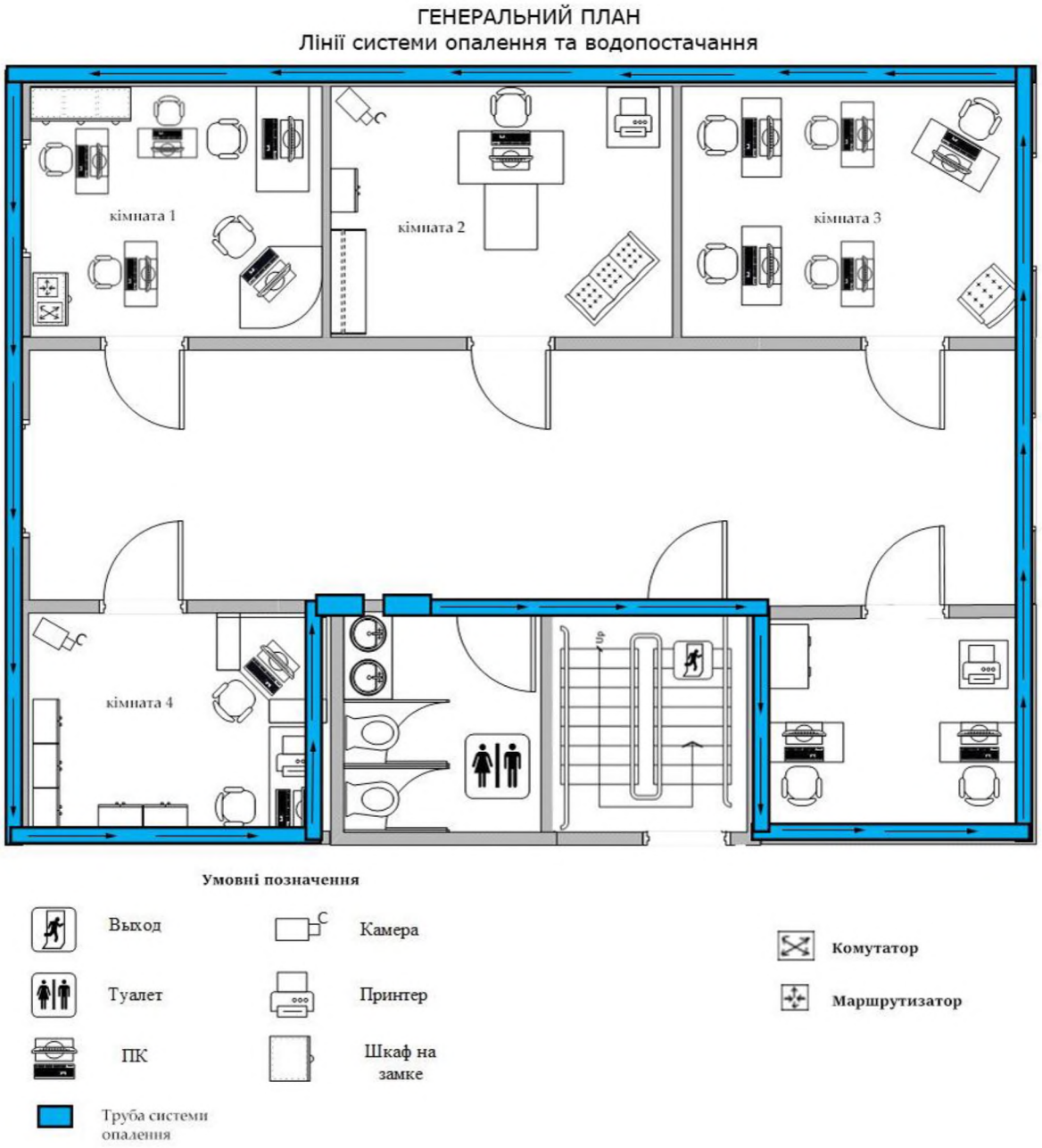

Рисунок 1.5. - Генеральний план. Лінії системи опалення та водопостачання

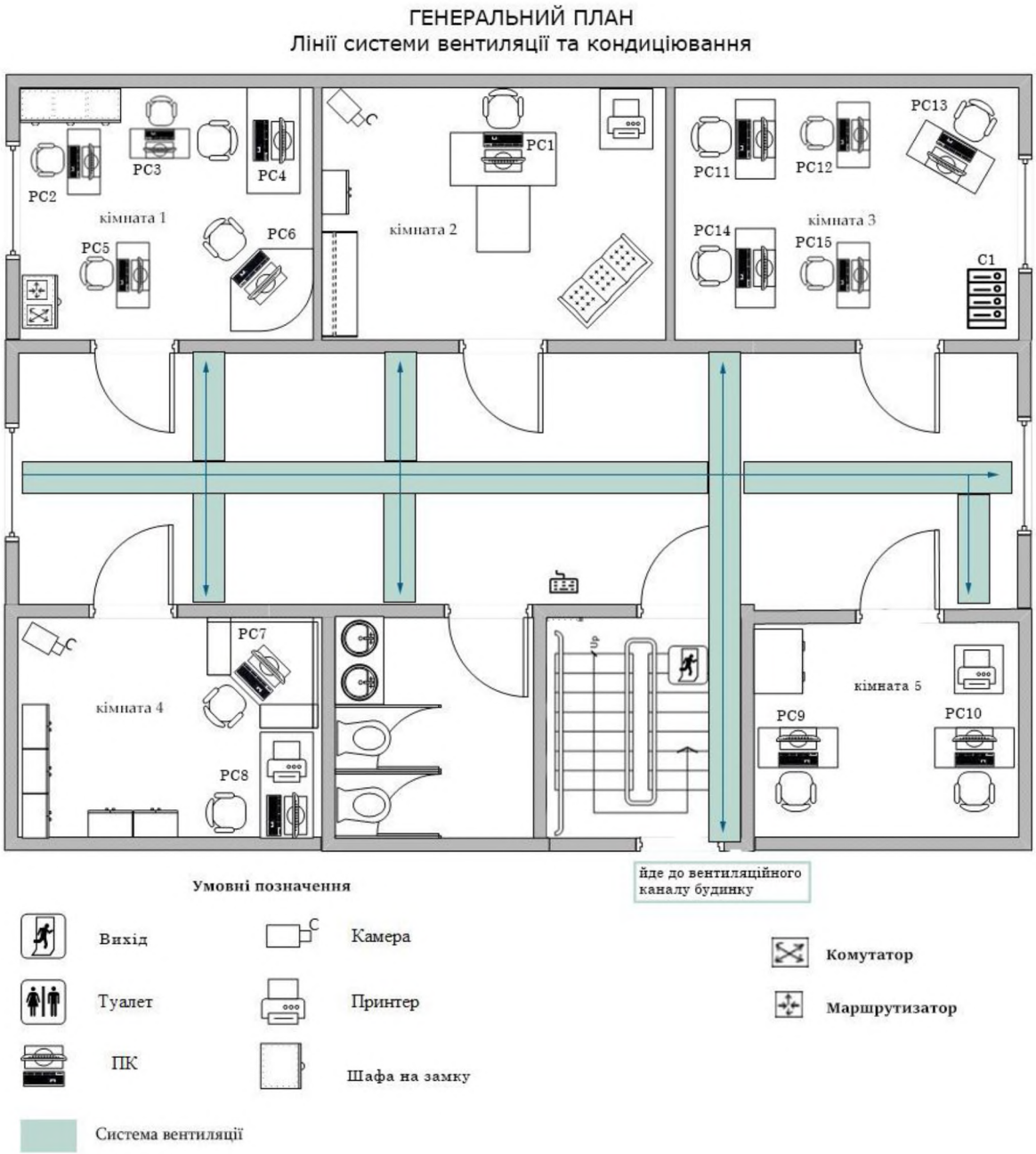

Рисунок 1.6. - Генеральний план. Лінії системи вентиляції та кондиціювання

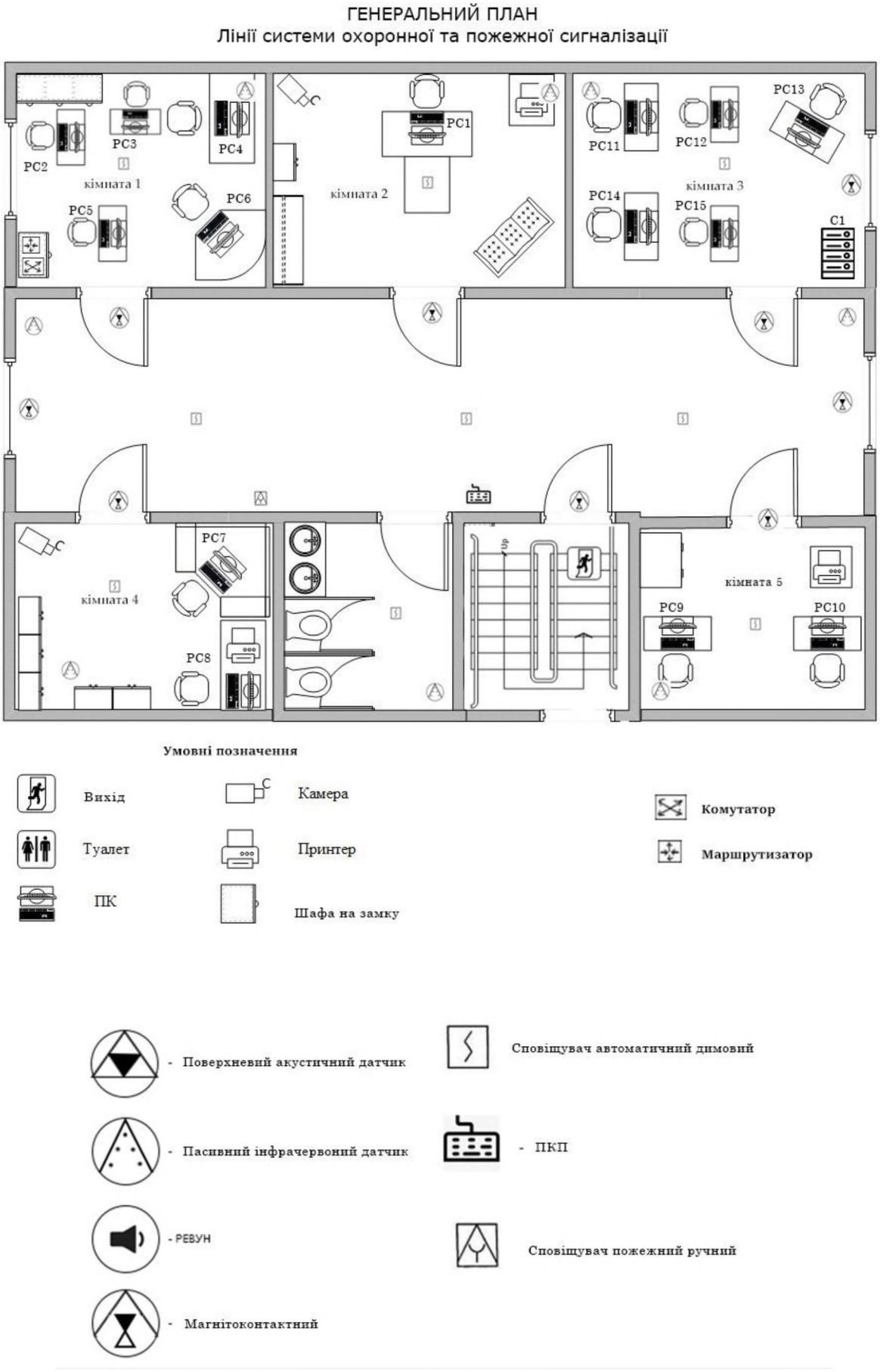

Рисунок 1.7. - Генеральний план. Системи охоронної та пожежної сигналізаці

1.3.2 Обстеження обчислювальної системи

На підприємстві є:

- десять комп'ютерів, які необхідні для роботи, вони зберігають в собі інформацію компанії;
- сервер, на який відбувається резервне копіювання документів з кожної робочої станції. Компанії використовують сервера для загального доступу всіх співробітників до певної інформації і для загального користування доступними ресурсами.
- Цей сервер вирішує проблеми стабільного загального доступу до однієї і тієї ж інформації. На цей же сервер раз на тиждень робиться резервна копія всіх файлів з усіх робочих станцій;
- два принтери з лазерним друком, які локально під'єднані до комп'ютерів системних адміністраторів;
- чотири веб-камери необхідні для того, щоб директор та менеджери з купівлі спілкувались за допомогою веб-камер з постачальниками;
- комутатор, який з'єднує десять комп'ютерів;
- маршрутизатор, який з'єднано з сервером та комутатором. Комп'ютери постійно мають доступ до сервера для отримання необхідної інформації.

На ОІД не має зовнішніх носіїв. Підприємство використовує хмарне сховище для обміну документів по мережі. У компанії відсутні політики, пов'язані із контролю інформаційного середовища.

Також у підприємства є власний клієнтський сайт, який зберігається на зовнішньому хостингу. Для обґрунтування формування вимог до КЗЗ ІТС, необхідно виконати її класифікацію згідно НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». АС на підприємстві відповідає ознакам класу 3. На рис. 1.8 представлена робоча група ОІД обчислювальна система відноситься до ОІД, що відносно невелику за масштабами

комп'ютерну мережу, створювану головним чином з метою забезпечення спільного доступу входять до неї РС до різних файлів.

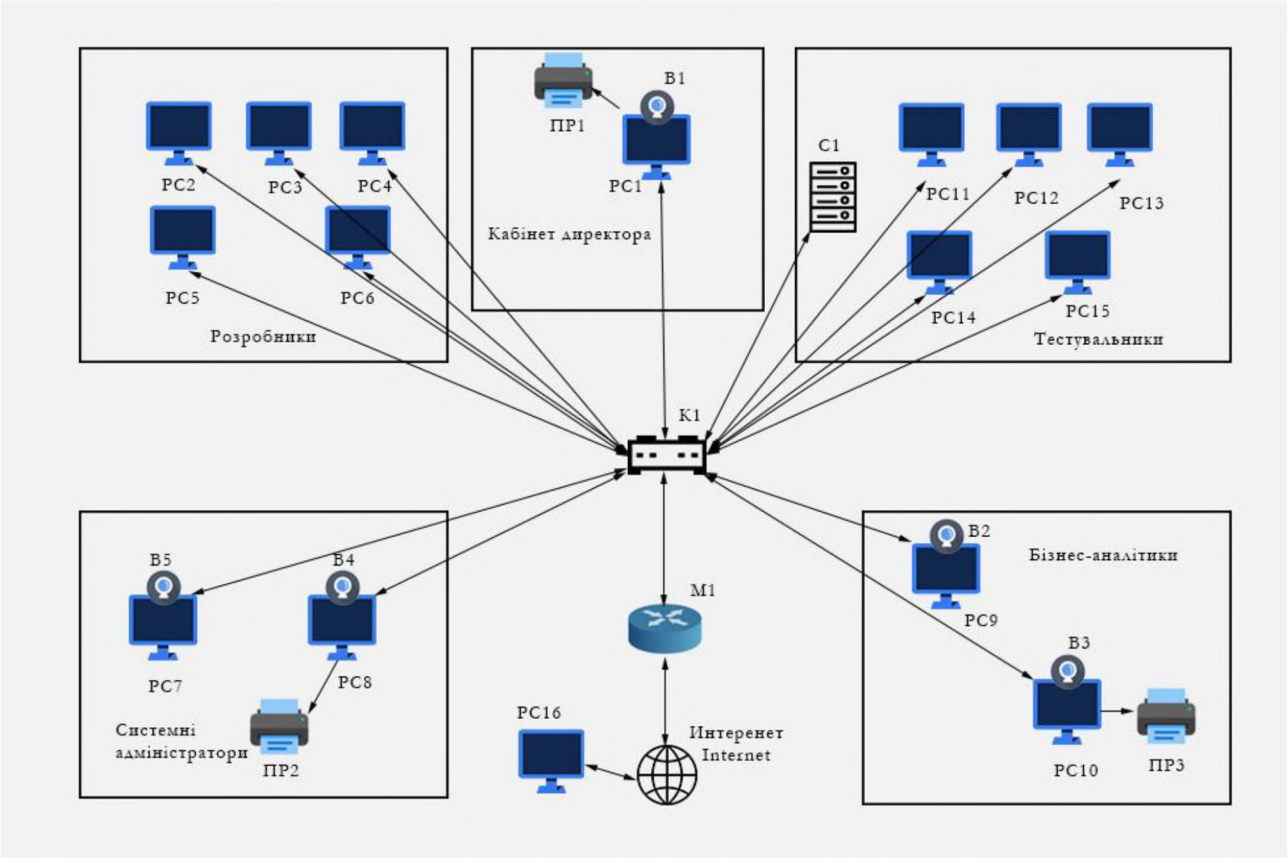

Рисунок 1.8. - Структурна схема ІТС

Доступ до системи можливий зазвичай тільки за умови, що операційна система РС буде завантажена з певного логіна (облікового запису користувача), для якого даний доступ відкритий і налаштований.

Всі РС об'єднані в локальну обчислювальної мережу з виходом в інтернет.

Табл. А.2 - Перелік апаратного забезпечення ІТС згідно з рис. 1.3 наведено у додатку А.

Табл. А.3 - Інвентаризаційна відомість ДТЗС наведена у додатку А.

1.3.3 Середовище користувачів

Обов’язки співробітників:

Головним на підприємстві є генеральний директор. У його повноваження входить управління підприємством, коригування робочих планів, надання

відпусток працівникам, прийняття нового персоналу на роботу, винесення рішень до зміни елементів офісу або підприємства, контроль проектів, планів та графіків.

Старший системний адміністратор – повинен підготовлювати і зберігати резервні копії даних, їх періодично перевіряти і знищувати, встановлювати і конфігурувати оновлення операційної системи і прикладного програмного забезпечення, встановлювати і конфігурувати нове апаратне і програмне забезпечення, створювати і підтримувати в актуальному стані файлу облікових записів користувачів, підтримувати інформаційну безпеку в організації, документування своєї работи, аналізувати трафіки співробітників під час роботи.

Системний адміністратор – повинен стежити за станом обладнання офісу, вчасно його обслуговування, оновлення систем та програмного забезпечення.

Бухгалтер – повинен вчасно робити податкові відомості, створювати щомісячні звіти підприємства, визначати заробітню плату відносно від процентної ставки співробітників, проводить аудити з керівником, щодо зміни цін певних послуг підприємства. Консультує генерального директора щодо зарплатні співробітників підприємства.

Бізнес-аналітик – шукають нових клієнтів, спілкується з клієнтами, створює план завдання за побажаннями клієнтів. Робить звіти за замовленням. Обговорюють питання стосовно продукту у дистанційній формі, передають інформацію до технічного відділу.

Розробник – технічне обслуговування та підтримка програм, що використовуються компанією і її клієнтами. Вивчають нові інструменти і механізми розвитку в середовищі хмарних обчислень.

Виконують технічне завдання клієнта, виправляють знайдені дефекти продукту, пишуть звіти про стан продукту, налаштовують середовище для роботи продукту, відправляють тестувальникам готову версію продукту.

Тестувальник – підготовляють і проводять тестування програм, виявляють помилки і похибки, які виникають при роботі з ПЗ та визначають причини їхнього виникнення, складають докладний письмового звіт про виконане тестування,

відправляють звіти бізнес-аналітикам та розробникам для подальшого виправлення помилок, налаштовують середовище автоматизації.

Рівень кваліфікації користувачів:

Високий: старший системний адміністратор, системний адміністратор, бізнес-аналітик.

Середній: генеральний директор, бухгалтер, розробник, тестувальник.

Табл. А.4 - Розмежування доступу до техніки матриця доступу наведено у додатку А.

Відповідальний за все обладнання – Старший та системний адміністратор.

Табл. А.5. - Інвентаризаційна відомість програмного забезпечення ІТС наведена у додатку А.

1.3.4 Оброблювана інформація і технології її обробки

На ОІД циркулює та обробляється така інформація: інформація про клієнтів компанії, та бухгалтерські звіти діяльності компанії, в якій є звіти з розробки продукту. Оброблюється інформація робочим персоналом компанії, яка включає в себе директора, системних адміністраторів , бізнес-аналітиків, 5 розробників та 5 тестувальників.

Інформація про клієнтів: ця інформація завантажується з ноутбуків бізнес-аналітика та директора, на сервер директором, бізнес аналітиком, з їх робочих станцій. Директор може копіювати цю інформацію.

Бухгалтерські звіти діяльності компанії: ця інформація завантажується з ноутбуків директора та бізнес-аналітиків на сервер директором та бізнес-аналітиками.

Бізнес-аналітик та директор можуть копіювати та друкувати цю інформацію, директор зберігає усю документацію на сервері та персональному комп'ютеру.

Проектна робота: ця інформація завантажується з комп'ютерів директора або бізнес-аналітика на сервер у вигляді ТЗ.

Співробітники, що тестують ПЗ використовують такі методи тестування:

Модульне тестування (Unit Testing) – це тип тестування програмного забезпечення, у якому тестуються окремі модулі чи компоненти програмного забезпечення.

Інтеграційне тестування – вид тестування, у якому відповідність вимог перевіряється інтеграція модулів, їх взаємодія між собою, і навіть інтеграція підсистем у одну загальну систему.

Black-box тестування – це функціональне та нефункціональне тестування без доступу до внутрішньої структури компонентів системи.

White-box тестування – метод тестування програмного забезпечення, який передбачає, що внутрішня структура системи відомі тестувальнику.

У відповідність до процесів або методологій розробки ПЗ, під час проведення тестування створюється і використовується певна кількість тестових артефактів:

1. План тестування (Test Plan) - це документ, що описує весь обсяг робіт з тестування, починаючи з опису об'єкта, стратегії, розкладу, критеріїв початку та закінчення тестування, до необхідного в процесі роботи обладнання, спеціальних знань, а також оцінки ризиків з варіантами їх вирішення.
2. Тест-кейси (Test Case) - це послідовність дій, за якою можна перевірити, чи відповідає функція, що тестується, встановленим вимогам.
3. Баг репорт (Bug Report) - це документ, що описує ситуацію або послідовність дій, що призвела до некоректної роботи об'єкта тестування, із зазначенням причин та очікуваного результату.
4. Чек-лист (Checklist) – список параметрів, який потрібно перевірити.

Таблиця 1.2 - Класифікація інформації, що циркулює в ОІД

№	Назва інформації	Вид представлення в ІТС	Правовий режим	Режим доступу	Вимоги до захисту		
					К	Ц	Д

№	Назва інформації	Вид представлення в ІТС	Правовий режим	Режим доступу	Вимоги до захисту		
					К	Ц	Д
1	Інформація про клієнтів	Графічна, текстова, числова	Відкритий	Відкрита	К2	Ц2	Д2

Продовження таблиці 1.2

2	Інформація про співробітників	Текстова, числова	Конфіденційна	Обмежений доступ	К1	Ц1	Д2
3	Бухгалтерські розрахунки	Текстова, числова	Конфіденційна	Обмежений доступ	К2	Ц2	Д2
4	Звіти тестувальників щодо стану продукту	Текстова, числова	Конфіденційна	Обмежений доступ	К2	Ц2	Д2
5	Звіти розробників щодо стану продукту	Текстова, числова	Конфіденційна	Обмежений доступ	К2	Ц2	Д2
6	Дані про розроблену продукцію компанії	Графічна, текстова, числова	Відкритий	Відкрита	К2	Ц2	Д2
7	Закази клієнтів, ТЗ	Текстова, числова	Конфіденційна	Обмежений доступ	К1	Ц1	Д2
8	Тестові артефакти	Текстова, числова	Конфіденційна	Обмежений доступ	К1	Ц2	Д2
9	Копії персональних даних співробітників	Текстова, числова	Конфіденційна	Обмежений доступ	К1	Ц2	Д2

К1 - Не призводить до розкриття конфіденційної інформації.

К2 - Призводить до розкриття окремих документів, які відносяться до “комерційної таємниці”, персональних даних і може призвести до незначних фінансових втрат.

К3 - Призводить до розкриття документів, які відносяться до “комерційної таємниці”, персональних даних і призводить до значних фінансових втрат, має значний вплив на репутацію підприємства.

Ц1 - Не призводить до фінансових втрат.

Ц2 - Призводить до незначних фінансових втрат та має незначний вплив на репутацію підприємства.

Ц3 - Призводить до великих фінансових втрат, має значний вплив на репутацію підприємства.

Д1 - Не впливає на доступність.

Д2 - На деякий час впливає на доступність до ресурсу, що може принести незначні збитки або мати невеликий вплив на репутацію підприємства.

Д3 - Унеможливлює користування ресурсом на тривалий час і має значний вплив на роботу підприємства.

Таблиця 1.3 - Матриця розмежування доступу

Об’єкт / Користувач	Кількість працівників	Інформація									Повноваження встановлювати ПЗ	Доступ до ресурсів
		1	2	3	4	5	6	7	8	9		
Генеральний директор	1	RW CD MSP	RW CD SP	RC DS P	RC DS P	RC DS P	RC DM SP	RC DM SP	RC DM SP	RW CDS P	+	PC PR SR
Бізнес-аналітик	2	RW CD MSP	RC SP	RC SP	RS	RC P	RW CD MS P	RC SP	RC SP	RW CD MSP	+	PC PR
Старший системни	1	RW CD	RW CD	RC DS	RC DS	RC DS	RC DM	RC DM	RC DM	RW CDS	+	PC PR

й адмін		MSP	SP	P	P	P	SP	SP	SP	P		SR
Системний адмін	1	RWCDMSP	RWCDSP	RCDSP	RCDSP	RCDSP	RCDMSP	RCDMSP	RCDMSP	RWCDSP	+	PCPR
Розробник	5	-	-	-	RCSP	RWCDMSP	RSP	RWCDMSP	RWCDMSP	RSP	+	PCPR

Продовження таблиці 1.3

Тестувальник	5	-	-	-	RWCDMSP	RCSP	RSP	RWCDMSP	RWCDMSP	RSP	+	PCPR
Бухгалтер	1	-	RC	RWCDMSP	-	-	RSP	-	-	RC	-	PCPR
Охоронець	1	-	RCSP	-	-	-	-	-	-	RC	-	PCPR

Примітка:

R – читання

W – запис (створення)

C – копіювання

D – видалення

M – модифікація

S – зберігання

P – друкування

PC – персональний комп’ютер

PR – принтер

SR – сервер

1.4 Аналіз порушників

Згідно із Наказу №141 від 20.07.2007 «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації»

Згідно НД ТЗІ 1.1-003-99 порушник - умовне позначення суб'єкта, який може навмисно чи ненавмисно здійснити несанкціоновані дії щодо інформації в системі.

Модель порушника являє собою сукупність поведінки суб'єкта, який може завадити роботі інформації в системі. Порушником може бути особа, яка являється співробітником підприємства, так і хакером або агентом конкуруючого підприємства чи іншою особою. Виходячи із описаних даних про підприємство, можна зробити припущення, що промисловий шпіонаж являється не рідким явищем.

Для визначення рівня загроз використаємо наступні таблиці: табл. 1.4, табл. 1.5, табл. 1.6, табл. 1.7, табл. 1.8, табл.1.9.

Таблиця 1.4 - Категорії порушників, визначених у моделі

Позначення	**Визначення категорії**	**Рівень загроз**
Внутрішні по відношенню до ІТС		
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС	1
ПВ3	Користувачі ІТС	2
ПВ4	Адміністратор ІТС(системний адміністратор)	3
ПВ5	Керівники різних рівнів(директор)	4
Зовнішні по відношенню до ІТС		
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання та інше)	2

ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів	4

Таблиця 1.5 - Специфікація моделі порушника за мотивами здійснення порушень

Позначення	**Мотив порушення**	**Рівень загроз**
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов'язок (ПЗ4)	4

Таблиця 1.6 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	**Основні кваліфікаційні ознаки порушника**	**Рівень загроз**
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 1.7. - Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	**Характеристика можливостей порушника**	**Рівень загроз**
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1

Позначення	**Характеристика можливостей порушника**	**Рівень загроз**
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 1.8 - Специфікація моделі порушника за місцем дії

Позначення	**Характеристика місця дії порушника**	**Рівень загроз**
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Таблиця 1.9 - Специфікація моделі порушника за часом дії

Позна-чення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час функціонування ІТС	1
Ч2	Під час бездіяльності компонентів системи (в неробочій час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.д.)	2
Ч3	Під час повної бездіяльності ІТС з метою відновлення та	3

	ремонту	
Ч4	Як у процесі функціонування систем захисту інформації, так і під час зупинки компонентів системи	4

ПВ - внутрішній порушник, варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов'язків.

ПЗ4 - зовнішній порушник, (агент конкурентів або закордонних спецслужб «під прикриттям») - варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації.

В табл. 1.10 наведена класифікація порушникі, що можуть бути в ІТС.

Найбільшу загрозу від внутрішніх співробітників мають системний адміністратор та розробник.

Таблиця 1.10 – Модель внутрішнього порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор	ПВ5	М3	К3	З3	Ч3	Д4	20
	4	3	3	3	3	4	
Головний системний адміністратор	ПВ4	М3	К4	З3	Ч4	Д4	21
	3	3	4	3	4	4	
Системний адміністратор	ПВ4	М3	К4	З3	Ч4	Д4	21
	3	3	4	3	4	4	
Бухгалтер	ПВ3	М3	К1	З3	Ч1	Д2	12
	2	3	1	3	1	2	
Розробник	ПВ3	М3	К3	З3	Ч1	Д2	14
	2	3	3	3	1	2	
Бізнес аналітик	ПВ3	М3	К3	З3	Ч1	Д2	14
	2	3	3	3	1	2	
Тестувальник	ПВ3	М3	К3	З3	Ч1	Д2	14

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
	2	3	3	3	1	2	

Таблиця 1.11 - Модель зовнішнього порушника

Категорія порушника «ПВ»	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Хакери	ПЗ3	М3	К4	З4	Ч1	Д3	18
Відвідувачи, сторонні особи	ПЗ1	М2	К1	З1	Ч1	Д1	7

Аналіз загроз для інформації в ІТС

Згідно НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу:

Модель загроз - абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні.

Типові види загроз для безпеки інформації:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);
- збої та відмови у роботі технічних або програмних засобів (далі - ПЗ) ІТС;
- наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);
- помилки персоналу (користувачів) ІТС під час експлуатації;
- навмисні дії (спроби) потенційних порушників.

Випадкові загрози суб'єктивної природи - це помилкові дії персоналу по неуважності, недбалості, незнанню тощо, але без навмисного наміру.

До них відносяться:

- дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм тощо);
- ненавмисне пошкодження носіїв інформації;
- неправомірна зміна режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);
- неумисне зараження ПЗ комп'ютерними вірусами;
- невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;
- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;
- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;
- неправомірне впровадження та використання заборонених політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення тощо);

- наслідки некомпетентного застосування засобів захисту тощо.

Навмисні загрози суб'єктивної природи – це дії порушника, спрямовані на проникнення в систему та одержання можливості НСД до її ресурсів або дезорганізацію роботи ІТС та виведення її з ладу.

До них відносяться:

- порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);
- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, кондиціонування тощо.);
- порушення режимів функціонування ІТС (обладнання і ПЗ);
- впровадження та використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;
- використання (шантаж, підкуп) з корисливою метою персоналу ІТС;
- крадіжки носіїв інформації, виробничих відходів (роздруків, записів);
- несанкціоноване копіювання носіїв інформації;
- читання залишкової інформації з оперативної пам'яті ЕОТ, зовнішніх накопичувачів;
- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача;
- неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;
- впровадження та використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);
- зберігання паперових документів бухгалтерії у звичайних шафах без можливості їх блокування або опечатування;

Збоку програмної та апаратної моделі загрози виникають через:

- підключення сторонніх носіїв інформації;

- пошкодження або відмова ліній резервного постачання ресурсів глобальної мережі;
- відсутність тимчасових паролів користувачів.

Таблиця 1.12 - Перелік загроз з визначенням порушень властивостей

№	Актуальні загрози для інформації в ІТС	Ризики для			
		К	Ц	Д	С
Антропогенні загрози					
1.	Неконтрольований друк	+			
2.	Ненавмисне відключення технічних ресурсів, відповідальних за збереження інформації (серверів, ПК тощо)		+	+	+

Продовження таблиці 1.12

3.	Читання даних, залишених без нагляду та читання даних, що виводяться на екран	+			
4.	Втрата доступу, через відсутність підключення до хмарного сховища			+	
5.	Втрата документів, або напрацювань через збої програмного і/або апаратного забезпечення		+	+	
6.	Зараження вірусами через встановлення програмного забезпечення	+	+	+	
7.	Несанкціоноване підключення до технічних засобів	+	+		+
8.	Несанкціоновані дії адміністратора або користувачів через неправильне налаштування журналу подій(системний адміністратор)				+
9.	Втрата паролів				+
10.	Втрата резервних копій з сервера		+	+	
11.	Несанкціоноване внесення змін у технічні засоби	+	+		
12.	Використання недозволеного програмного			+	+

	забезпечення або модифікація компонентів програмного та інформаційного забезпечення.				
13.	Пошкодження носіїв інформації(сервер, жорсткий диск)		+	+	
14.	Вхід в систему недопущених осіб (подолання систем захисту)	+	+	+	
15.	Відстутність доступу до хмарного сховища			+	
16.	Втрата копій документів або коду через неправильне налаштування резервного копіювання		+	+	
17.	Несанкцоновані дії через неправильне налаштування прав доступу співробітників	+	+	+	

Продовження таблиці 1.12

18.	Несанкціоноване ознайомлення або пошкодження через неправильне зберігання документів	+	+		
19.	Несанкціонований доступ до системи та інформації через неправильно налагоджена система сигналізації	+	+		
20.	Відсутність шифрування даних	+			
21.	Перехоплення важливих документів через незахищений канал зв’язку.	+			
22.	Взлом системи через фішинг	+	+		
23.	Використання заборонених ресурсів Інтернету	+			
24.	DDos-атака нашої продукції(сайти та додатки)			+	+
Техногенні загрози					
1.	Відсутність електропостачання		+	+	
2.	Збій обчислювальної техніки		+	+	
3.	Збій програмного забезпечення	+	+	+	

1.6 Висновки до 1 розділу

Повертаючись до даного розділу, був описаний ОІД :

- загальна інформація про підприємство;
- опис інформаційної системи;
- опис обчислювальної сиситеми;
- опис користувачів системи та їх дозвіл до інформації в АС;
- загальна інформація про інвентар в офісі;

Також було проаналізовано джерела загроз і вразливостей, на основі цього аналізу ми можемо вводити КЗЗ, щоб надати методи та засоби захисту інформації в ІТС. Розроблені моделі порушників та моделі загроз.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА.

2.1 Визначення рівня реалізації послуг безпеки

При створені КСЗІ виникає необхідність у формалізації вимог щодо спроможності системи забезпечувати захист інформації. Це необхідно при розробці технічного завдання та при випробуваннях системи. Ці вимоги можливо розділити на два напрями:

- захист оброблюваної інформації від несанкціонованого доступу;
- захист оброблюваної інформації від витоку технічними каналами.

В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

- вимоги до функцій захисту (послуг безпеки);
- вимоги до гарантій.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз.

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, існують критерії гарантій, що дозволяють оцінити коректність реалізації послуг.

Таким чином, Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Слід зазначити, що більшість критеріїв взаємопов’язані між собою. Тобто, для реалізації деяких Критеріїв необхідною умовою є виконання інших.

Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу наведено в НД ТЗІ 2.5-004-99.

Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу наведено в НД ТЗІ 2.7 -009-09.

Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу наведено в НД ТЗІ 2.7-010-09.

2.2 Визначення вимог до захисту КЗЗ

Сформовані вимоги до критеріїв захисту інформації, наведено у табл. 2.1.

Таблиця 2.1 – Вимоги до критеріїв захисту інформації

Критерії	Послуги безпеки	Вимоги до рівня послуг безпеки
Конфіденційність	Довірча конфіденційність	КД-2 –Базова довірча конфіденційність
	Адміністративна конфіденційність	КА-2 – Базова адміністративна конфіденційність
	Повторне використання об’єктів	КО-1 – Повторне використання об’єктів

Критерії	Послуги безпеки	Вимоги до рівня послуг безпеки
	Конфіденційність при обміні	КВ-2 –Базова конфіденційність при обміні
Цілісність	Довірча цілісність	ЦД-1 − Мінімальна довірча цілісність
	Відкат	ЦО-1 − Обмежений відкат
	Цілісність при обміні	ЦВ-2 – Базова цілісність при обміні
Доступність	Використання ресурсів	ДР-1 − Квоти
	Відновлення після збою	ДВ-1 − Ручне відмовлення

Продовження таблиці 2.1

Спостереження	Реєстрація	НР-2 − Захищений журнал
	Ідентифікація і автентифікація	НИ-1 – Зовнішня ідентифікація і автентифікація
	Достовірний канал	НК-1 − Однонаправлений достовірний канал
	Розподіл обов’язків	НО-2 − Розподіл обов’язків адміністраторів
	Цілісність комплексу засобів захисту	НЦ-2 − КЗЗ з гарантованою цілісністю
	Ідентифікація та автентифікація при обміні	НВ-1 − Автентифікація вузла

Спостереження	Реєстрація	НТ-2 – Самотестування при старті
Гарантії	Рівень гарантій	Г-2

2.3 Профіль захищеності

2.3.1 Обґрунтування вибору

Для даного підприємства можна визначити необхідний профіль захищеності, цим профілем є 3.КЦД.2.

3.КЦД.2 = {КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}, Г-2

2.3.2 Опис профілю захищеності

Визначаючи вимоги до КЗЗ було вирішено розділити об’єкти на множини, що потребують захисту.

Множина об’єктів 1: інформація на сервері С1 копії множини 2 та первинний код.

Множина об’єктів 2: інформація про клієнтів, звіти щодо стану розробки продукту, програмний код, ТЗ, копії персональних даних, бухгалтерські звіти, документи ЗЕД (все міститься на жорстких дисках комп’ютерів та на сервері С1).

Множина об’єктів 3: ПЗ, що встановлено, всі технологічні файли, що зберігаються на робочих станціях та на сервері С1.

Опис умов:

- КД-2 - Базова довірча конфіденційність

Необхідні умови: НИ-1

Ця послуга відноситься до множини об’єктів: 3

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Користувач отримує доступ до програм (Microsoft SQL Server (від 2019), Microsoft Visual Studio, доступ до облікового запису в системі, С1) при реєстрації користувача в системі, змінити права можливо лише на підставі атрибутів доступу.

- КА-2 – Базова адміністративна конфіденційність

Необхідні умови: НО-1, НИ-1

Ця послуга відноситься до множини об’єктів: 2

КЗЗ повинен надавати можливість головному адміністратору, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

Головний адміністратор керує потоками інформації від захищених об’єктів до користувачів, що є в ІТС (наприклад доступ до розробки продукту, тобото доступ до середовища розробки або тестування).

- КО-1 – Повторне використання об’єктів

Необхідні умови: НЕМАЄ

Множина об’єктів: оперативна пам’ять комп’ютерів та пам’ять на сервері С1

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

- КВ-2 – Базова конфіденційність при обміні

Необхідні умови: НО-1

Ця послуга відноситься до множини об’єктів: електронна пошта,

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем

захищеності. КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Задля того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, слід надати певні послуги захисту інформації в системі. Слід заборонити модифікувати інформацію, що циркулює в ІТС. Цілісність забезпечується такими послугами:

- довірча цілісність,
- адміністративна цілісність,
- відкат,
- цілісність при обміні.

- ЦД-1 – Мінімальна довірча цілістність

Необхідні умови: НИ-1

Ця послуга відноситься до множини об’єктів: 1, 2

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт.

- ЦА-2 – Мінімальна адміністративна цілісність

Необхідні умови: НО-1, НИ-1

Ця послуга відноситься до множини об’єктів: 3

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта. КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт.

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес(цим займається головний системний адміністратор).

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

- ЦО-1 – Обмежений відкат

Необхідні умови: НИ-1

Ця послуга відноситься до множини об’єктів: 1, 2, 3

Головний системний адміністратор повинен визначити, які об’єкти або операції можуть бути відкачені. Автоматизовані засоби повинні надавати користувачу можливість відкатити те, до чого він має доступ за певний проміжок часу.

- ЦВ-2 – Базова цілісність при обміні

Необхідні умови: НО-1

Ця послуга відноситься до множини об’єктів: 2

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається а також фактів його видалення або дублювання.

Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

Захищає інформацію від модифікації при імпорті/експорті через незахищене середовище. Головний адміністратор бачить усі модифікації та може це контролювати.

Задля того, щоб КС могла бути оцінена на предмет відповідності критеріям доступності, слід надати певні послуги захисту інформації в системі. Слід забезпечити можливість використання КС в цілому або окремих її об'єктів, або окремих функцій, або циркулюючої інформації в ІТС в заданий час. КЗЗ повинна надати можливість КС функціонувати у випадку відмови деяких компонентів. Доступність забезпечується такими послугами:

- використання ресурсів,
- стійкість до відмов,
- гаряча заміна,
- відновлення після збоїв.

- ДР-1 – Квоти

Необхідні умови: НО-1

Ця послуга відноситься до множини об'єктів: простір на диску,сервері.

Квоти – обмеження можливостей користувачів, щоб не було зроблено копій, щоб не стала система.

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від

користувачів, яким надані відповідні повноваження

Користувачі можуть керувати послугами та використовувати ресурси.

- ДВ-1 – Ручне відновлення

Необхідні умови: НО-1

Ця послуга відноситься до множини об'єктів: системне або прикладне ПЗ

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе

повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС. Після відмови КС або переривання

обслуговування КЗЗ повинен перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі,

яким надані відповідні повноваження.

Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування.

Ця послуга дає можливість КС повернутися до захищеного стану після відмови або збою.

Задля того, щоб КС могла бути оцінена на предмет відповідності критеріям спостережності, слід надати певну відповідальність користувачів за свої дії та за допомогою спроможності КЗЗ виконувати свої обов'язки. Спостережність забезпечується такими послугами:

- реєстрація (аудит),
- ідентифікація і автентифікація,
- достовірний канал,
- розподіл обов'язків,
- цілісність КЗЗ,
- самотестування,
- ідентифікація і автентифікація при обміні,
- автентифікація відправника,
- автентифікація отримувача.

- НР-2 – Захищений журнал

Необхідні умови: НИ-1, НО-1

КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки:

- вхід/вихід до системи;
- друк;

- відмова у доступі ;
- дата;
- кількість підписів;
- доступ до файлів;
- створення/видалення облікового запису
- оновлення ПЗ;
- протоколи TCP, HTTP.

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Головний адміністратор може контролювати небезпечні для КС дії.

- НИ-2 – Одиночна ідентифікація і автентифікація

Необхідні умови: НЕМАЄ

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ.

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача.

Найважливіша умова, завдяки якій стає можливою реалізація багатьох інших умов захисту інформації. Дозволяє автентифікувати та ідентифікувати користувача, що намагається здобути доступ до КС.

- НК-1 – Однонаправлений достовірний канал

Необхідні умови: НЕМАЄ

Користувач може взаємодіяти з КЗЗ напряму. Повноваження визначаються залежно від надання можливості ініціацій захищеного обміну.

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ.

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

- НО-2 – Розподіл обов'язків адміністратора

Необхідні умови: НИ-1

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки(в системі це головний системний адміністратор) та іншого адміністратора(системний адміністратор).

Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

- НЦ-2 – КЗЗ з гарантованою цілісністю

Необхідні умови: НЕМАЄ

Ця послуга відноситься до: реєстр, системні файли, програми.

Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів.

КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування.

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

КЗЗ повинно захищати себе та мати спроможність керувати захищеними об’єктами. Це робиться за допомогою автоматичної перевірки та оновлення баз, та брандмауеру Windows 10.

- НТ-2 – Самотестування при старті

Необхідні умови: НО-1

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

КЗЗ гарантує правильність функціонування та цілістність певного списку функцій в КС після самотестування на старті.

- НВ-1 – Автентифікація вузла

Необхідні умови: НЕМАЄ

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму.

Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

Послуга потрібна, щоб забеспечити роботу між двома КЗЗ Їхня ідентифікація, перевірка ідентичності, це може робити як перша, так і друга КЗЗ. Це може статися при оновленні ПЗ.

2.3.3 Аналіз ступеня реалізації

В результаті аналізу КС було виявлено:

- реалізовані послуги: КД-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НИ-2.
- частково реалізовані: КВ-2.

- нереалізовані: КА-2, НО-2, НР-2, НЦ-2, НТ-2 , НК-1, НВ-1.

Головному системному адміністратору і системному надаються різні права, що зменшить потенційні збитики від навмисних або помилкових дій користувачів, також це обмежить авторитарність керування.

2.4 Проектні рішення

Для реалізації розмежування доступу, тобто КА-2, системному адміністратору необхідно розмежувати об'єкти захисту, що містять ІзОД, за атрибутами доступу користувачів згідно нової матриці доступу(табл. 2.1) Це можна зробити в локальній політиці безпеки ОС Windows 10.

Для реалізації НО-2 необхідно розділити обов’язки головного системного адміністратора та директора підприємства. При однакових правах двох адміністраторів неможлива реалізація профілю захищеності.

Для реалізації НР-2 головному системному адміністратору необхідно включити аудит подій безпеки, що зображено на рис. 2.1 та налаштувати події, які потрібно зареєструвати:

автентифікація користувача, використання зовнішніх носіїв, зміна атрибутів доступу, запуск ПЗ, встановлення та оновлення ПЗ, збої активації корпоративної ліцензії, збої перевірки сертифікату сайту, виведення документів на друк.

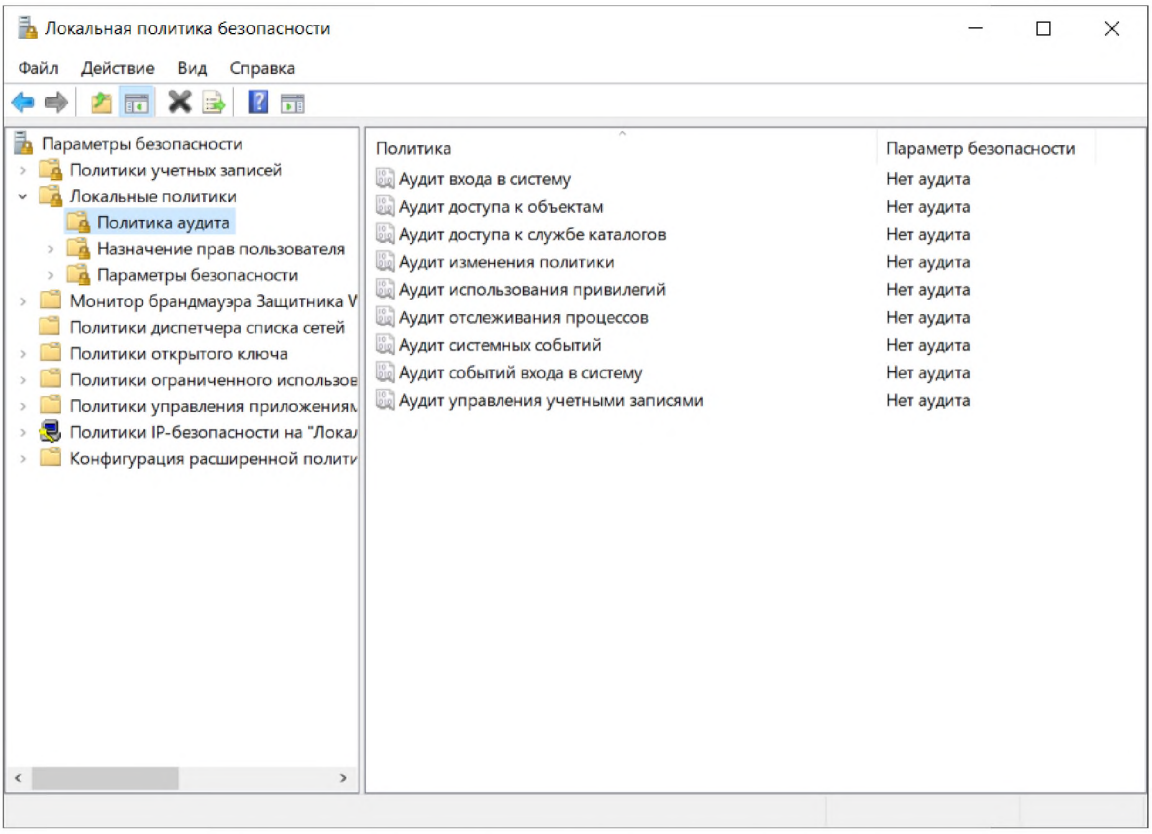

Рисунок 2.1 – Налаштування журналу подій

Для реалізації НЦ-2 необхідно від імені адміністратора у ОС Windows встановити налаштування “Контроль цілісності”, як показано на рис. 2.2.

В Windows 10, всі учасники безпеки (користувачі, комп'ютери, служби тощо) і об'єкти (файли, ключі реєстру). , папки та ресурси) отримують мітки MIC.

Обов'язковий контроль цілісності (MIC) забезпечує механізм контролю доступу до об'єктів, що захищаються, і допомагає захистити вашу систему від шкідливого інтернету.

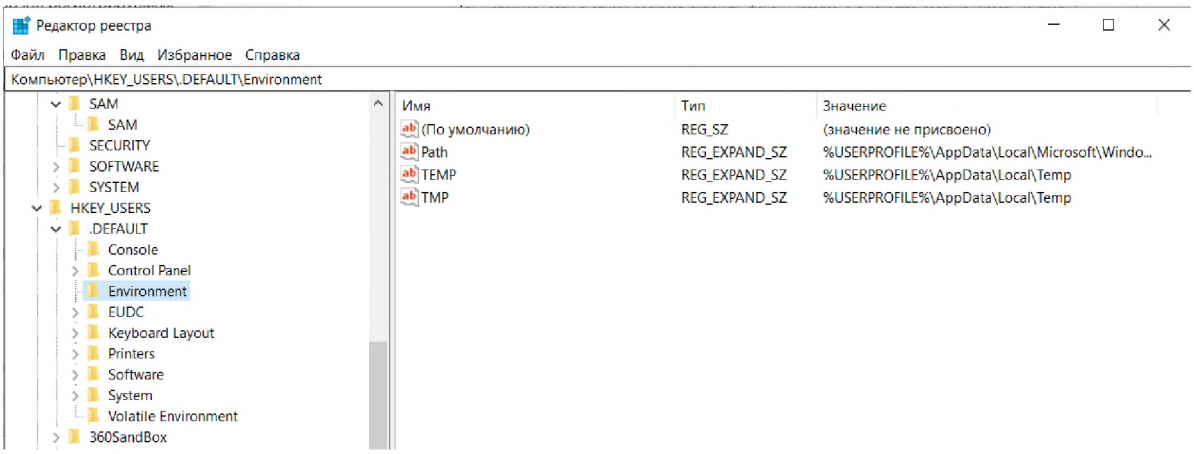

Рисунок 2.2 – Налаштування контролю цілісності через редактор реєстра

При цьому ОС буде контролювати цілісність системних та програмних файлів шляхом їх неможливого змінення, навіть від імені адміністратора. Цей механізм захисту не буде давати змогу оновлювати ПЗ за вимогою.

При необхідності оновити ПЗ, а це означає змінити системні та програмні файли, необхідно буде вимкнути дану функцію у налаштування ОС Windows, після цього провести оновлення ПЗ та включити функцію знову для контролю цілісності.

Для реалізації НТ-2 необхідно у налаштуваннях BIOS ввімкнути само тестування при старті, але ця функція є не надійною через те, що вона тестує елементи до завантаження системи.

Самотестування після старту ОС можна реалізувати наступними програмами: AIDA64, MSI Afterburner, Sandra 20/20. Для цього необхідно встановити їх на ПК та налаштувати на самоаналіз при старті, можливе доповнення тестування у встановлений час та збереження звітності з тестування систем для аналізу системним адміністратором.

На підприємстві кожен співробітник може увійти у свій обліковий запис з будь-якого ноутбука, який раніше був авторизованим у мережі підприємства. Вхід до системи дозволяється при спів падінні логіну та паролем.

Логіни та паролі співробітників зберігаються на сервері у хешованному вигляді. Доступ до даної інформації можливий лише головному системному адміністратору підприємства, системному адміністратору та керівнику підприємства.

Після входу в систему визначаються можливості користувача або адміністратора, його можливий доступ до сервера та певних файлів системи та виробництва. Вся інформація підприємства розподілена на “гілки” у сховищі даних, кожному користувачеві надається можливість відкривати лише ті “гілки”, які йому необхідні при роботі.

Система робить резервне копіювання у стиснутому вигляді до сервера компанії кожний понеділок та п’ятницю.

Самотестування системи відбувається при запуску її за допомогою BIOS та за вимогою адміністратора спеціальним ПЗ.

Аналіз системи на захищеність відбувається у реальному часі за допомогою антивірусних програм та ПЗ що дозволяє слідкувати за інформаційними потоками підприємства.

Також для цього у системі відбувається моніторинг журналу подій. За цим можуть слідкувати головний системний адміністратор та системний адміністратор.

За розподіл ресурсів відповідає ОС Windows, яка автоматично перенаправляє потужності на необхідні процеси при роботі з ПК.

Шифрування даних (КВ-2) реалізовано лише для зв'язку з банком, тому що він надає захищений канал зв'язку зі своїми ресурсами.

Так як підприємство працює з Американськими клієнтами, вони вимагають шифрування за їхніми стандартами та використання їхнього VPN.

Для забезпечення однонаправленого достовірного каналу та автентифікації вузла (НК-1, НВ-1) також рішенням є встановлення VPN.

Для забезпечення зв'язку ще з замовниками, що знаходяться в іншій країні, треба встановити VPN та обміном даними з сервером підприємства, реалізовується більшість норм з використання, зберігання, обробки і передачі інформації

2.4.1 Елементи політики безпеки

Працівники повинні відкривати підозрілу пошту тільки в віртуальній машині, відкриваючи вкладення електронної пошти, отримані від невідомих відправників, які можуть містити шкідливе програмне забезпечення.

В результаті аналізу середовищ функціонування ІТС і моделі загроз було виявлено, що матриця надлишкова. Нова матриця наведена у табл. 2.1

Була змінена матриця розмежування доступу.

Таблиця 2.2 – Нова матриця розмежування доступу

Об'єкт	Ki	Інформація	П ов	Д о

Користувач		1	2	3	4	5	6	7	8	9		
Генеральний директор	1	RS	RS	RS	RS	RS	RCDMSP	RS	RS	RWCDSP	+	PCPRSR
Бізнес-аналітик	2	RWCDMSP	RCSP	RCSP	RS	RCP	RWCDMSP	RCSP	RCSP	RWCDMSP	-	PCPR
Старший системний адмін	1	R	RCSP	R	R	RSP	RSP	RSP	RSP	RSP	+	PCPRSR
Системний адмін	1	-	RCSP	R	R	RSP	RP	RP	RP	RP	+	PCPR
Розробник	5	-	-	-	RCSP	RWCDMSP	RSP	RWCDMSP	RWCDMSP	RSP	-	PCPR
Тестувальник	5	-	-	-	RWCDMSP	RCSP	RSP	RWCDMSP	RWCDMSP	RSP	-	PCPR

Продовження таблиці 2.2

Бухгалтер	1	-	-	RWCDMSP	-	-	R	-	-	R	-	PCPR

Охороне ць	1	-	RC SP	-	-	-	-	-	-	RC	-	PC PR

2.4.2 Політика паролів

Суворі паролі, довгі, чим більше символів у вас є, тим сильніший пароль. Ми рекомендуємо використовувати в паролі щонайменше 14 символів. Крім того, ми рекомендуємо використовувати паролі, що складаються з декількох слів. Як приклади можна назвати "Час відпочинку" або "блок-схеми-спуни-листи".

Паролі легко запам'ятовуються та друкуються, але водночас задовольняють вимоги щодо міцності.

Погані або слабкі паролі мають такі характеристики:

- Містять не більше восьми символів.
- Містить особисту інформацію, таку як дати народження, адреси, номери телефонів або імена членів сім'ї, домашніх тварин, друзів та фантастичних персонажів.
- Містить шаблони номерів, такі як aaabbb, qwerty, zyxwvuts або 123321.
- Деякі версії "Welcome123" "Пароль123" "Gfhjkm123".

Крім того, кожен робочий обліковий запис повинен мати свій унікальний пароль. Для того, щоб користувачі могли підтримувати кілька паролів, ми настійно рекомендуємо використовувати програмне забезпечення "password manager", яке авторизоване та надається організацією. Якщо це можливо, також увімкніть багатофакторну автентифікацію.

Паролі системного та користувацького рівня мають відповідати Політиці паролів. Забороняється надавати доступ іншій особі навмисно або через недопущення забезпечення доступу.

Усі комп’ютерні пристрої мають бути захищені за допомогою паролем заставки з функцією автоматичної активації на 10 хвилин або менше. Ви повинні заблокувати екран або вийти з системи, коли пристрій без нагляду.

2.4.3 Необхідне ПЗ

ПЗ яке необхідно впровадити для захисту підприємства:

- 360 Total Security - антивірусна програма яка є складовою ОС, проводить активну перевірку одержаних файлів, робить аналіз системи і не потребує втручання спеціалістів.
- WireShark - програма для стеження пакетів даних, які відправляються та надходять до комп'ютерів та серверів. Зручна у вивчені та користуванні.
- VPN CyberGhost - VPN створює захищене з'єднання між ПК та глобальною мережею, захищає від стеження за трафіком та стороннього втручання. Ця програма має зручні пакети налаштувань, а саме підключення при запуску ПК та сервера, має зрозумілий інтерфейс та високу швидкість при навантаженнях, зручне ПЗ для використання у широких масштабах.

Програму WireShark використовує лише головний системний адміністратор та системний адміністратор підприємства. За допомогою фільтру програми він може стежити як за всіма пакетами які надходять та виходять з підприємства, так і за певними пакетами або певними ПК. При перехопленні пакетів спеціаліст аналізує їх зміст, посилання на сторонні вебсторінки, вид інформації що надсилається, тощо.

У разі необхідності можливе відключення від мережі для запобігання перехоплення інформації з сторонніх каналів зв'язку.

Антивірусна програма 360 Total Security - встановлена на всіх ПК підприємства, вмикається зі стартом системи, забезпечує активний захист ПК у реальному часі, серед приємних бонусів безкоштовного антивірусного ПЗ є моніторинг завантажень файлів та системи, активне блокування шкідливих сайтів та реклами, безпосередній вплив шпигунського та шкідливого ПЗ шляхом видалення або переміщення у карантин, оголошення про стан системи користувачеві кожен раз коли необхідні дії з системою.

VPN CyberGhost - встановлений на кожному ПК підприємства, він починає працювати при старті системи, тому користувачам не потрібно вмикати його самостійно. Якщо програма не зможе встановити зв'язок з серверами, вона повідомить про це користувача, який зможе самостійно натиснути кнопку "з'єднання" та самостійно вирішить цю проблему.

2.4.4 «Гриф-Мережа» версії 4.

Рішенням реалізації послуг безпеки може виступати КЗЗ «Гриф» версії 4, його можна використовувати як на комп'ютерах, так і на серверах. Він буде встановлений на комп'ютері головного системного адміністратора.

Згідно офіційного сайту Інституту комп'ютерних технологій комплекс «Гриф» реалізовує такі функції:

Комплекс «Гриф» версії 4 реалізує такі основні функції захисту:

- ідентифікацію та автентифікацію користувачів на підставі імені (псевдоніма), пароля та персонального носія даних автентифікації (дискети, пристрою Flash Drive, CD-RW, DVD-RW або іншого знімного файлового носія);

- розподіл обов'язків користувачів та виділення декількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрацію захищених ресурсів, реєстрацію користувачів, призначення прав доступу, оброблення протоколів аудиту, тощо);

- розмежування доступу користувачів до обраних каталогів файлової системи незнімних носіїв ПЕОМ (у тому числі різних ПЕОМ, що функціонують у складі ЛОМ) та файлів, що містяться у них, що дозволяє організувати спільну роботу декількох користувачів, які мають різні службові обов'язки та права по доступу до захищеної інформації;

- курування потоками інформації та блокування потоків інформації, що можуть призвести до зниження її рівня конфіденційності;

- керування створеними на знімних або незнімних носіях ПЕОМ захищеними логічними дисками, вся інформація на яких зберігається у зашифрованому вигляді, та розмежування доступу до їх вмісту з використанням механізмів "прозорого" розшифрування/ зашифрування даних у момент їх читання/ запису, що дозволяє забезпечити захист конфіденційності збереженої інформації навіть у випадку крадіжки ПЕОМ або відповідних носіїв;

- контроль цілісності захищених логічних дисків, що дозволяє забезпечити захист від несанкціонованої модифікації збереженої на них інформації при відключених засобах захисту або у випадку крадіжки відповідних носіїв;

- контроль за виведенням інформації на пристрої друку з можливістю маркування друкованих аркушів документів (у форматі "Office Open XML") відповідно до вимог діючих нормативних документів в сфері охорони державної таємниці;

- контроль за експортом інформації на знімні носії та за імпортом інформації зі знімних носіїв із забезпеченням можливості реєстрації змінних носіїв та обмеження (для певних користувачів) переліку використовуваних знімних носіїв тільки зареєстрованими;

- гарантоване знищення інформації з обмеженим доступом при видаленні відповідних файлів;

- розмежування доступу прикладних програм до обраних каталогів та файлів, що містяться у них, що дозволяє забезпечити захист інформації від випадкового видалення або пошкодження, а також забезпечити дотримання технології її оброблення;

- контроль цілісності прикладного програмного забезпечення та ПЗ комплексу, а також блокування завантаження програм, цілісність яких порушено, що дозволяє забезпечити захист від шкідливих програм (комп'ютерних вірусів) та дотримання технології оброблення ІзОД;

- контроль за використанням дискового простору користувачами, що виключає можливість блокування одним із користувачів можливості роботи інших користувачів;

- можливість блокування пристроїв інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;

- контроль цілісності та самотестування комплексу при старті та за запитом адміністратора;

- відновлення функціонування комплексу у випадку збоїв, що гарантує доступність інформації при дотриманні правил доступу до неї;

- реєстрацію, аналіз та надання уповноваженим адміністраторам можливості оброблення інформації про події, які мають безпосереднє відношення до безпеки оброблюваної інформації, що дозволяє адміністраторам контролювати доступ до

ІзОД, слідкувати за тим, як використовується комплекс, а також правильно його конфігурувати;

- ведення архівів зареєстрованих даних аудита;

- взаємодію з прикладними програмними системами (ППС) через визначений розробником комплексу інтерфейс, що дозволяє забезпечити безперервність захисту ІзОД при її обробці як штатними засобами ОС, так і засобами різноманітних ППС.

Отже, сукупність функцій та механізмів захисту інформації, реалізованих в комплексі «Гриф» версії 4, забезпечує реалізацію такого функціонального профілю захищеності:

{КА-2, КО-1, ЦА-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-3, НИ-3, НК-1, НО-2, НЦ-2, НТ-2}

Таблиця 2.2 – Порівняльна характеристика вимог захищеності

Вимоги захищеності інформації	КЗЗ «Гриф-Мережа»
КА-2	КА-2
НО-2	НО-2
НР-2	НТ-2
НЦ-2	НЦ-2
НТ-2	НТ-2
КВ-2	-
НК-1	НК-1
НВ-1	-

З табл. 2.2 можна зробити висновок, що КЗЗ «Гриф» версії 4 частково реалізує необхідні вимоги.

2.7 Висновки до 2 розділу

У другому розділі був проведений аналіз існуючих вимог захищеності інформації та визначено проектні рішення.

Для забезпечення захисту інформації були реалізовані наступні рішення:

- нова матриця доступу;
- визначені програми захисту інформації та інструкції до них;

реалізвані вимоги захищеності інформації за допомогою вбудованих функцій Windows 10 та КЗЗ «Гриф» версії 4 та встановлення допоміжних програм:

- 360 Total Security,
- WireShark,
- VPN CyberGhost.

Економічну доцільність можна побачити в 3 розділі.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ.

Основною метою даного розділу є обґрунтування економічної доцільності реалізації КСЗІ для ТОВ «Українські Інноваційні Технології», прорахунок всіх витрат на реалізацію КСЗІ в ІТС та надання рекомендацій стосовно зниженню витрат на створення і підтримку КСЗІ.

У наступних підрозділах буде розглянуто витрати організації на розробку

КСЗІ. Умовно, задачу можна розподілити на декілька етапів:

- розрахунок капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забеспечення;
- розрахунок річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування;
- визначення річного економічного ефекту від впровадження об'єкта проектування;
- визначення та аналіз показників економічної ефективності запропонованого в дипломному проекті проектного рішення;
- висновок.

3.1 Розрахунок капітальних витрат

До капітальних витрат належать витрати на розробку заходів із забезпечення інформаційної безпеки, а також витрати на придбання матеріальних та нематеріальних активів.

3.1.1 Визначення трудомісткості розробки КСЗІ

Тривалість кожної робочої операції порахуємо згідно формули (3.1)

$$t = \text{tтз} + t\text{в} + t\text{а} + t\text{вз} + t\text{озб} + t\text{овр} + t\text{д}, \text{годин} \quad (3.1)$$

де $t_{тз}$ - час на оформлення технічного завдання, (Всього: 14 год);

$t_в$ - час розробки концепції безпеки інформації організації, (Всього: 8 год);

$t_а$ - тривалість процесу аналізу ризиків, (Всього: 20 год);

$t_{вз}$ - тривалість визначення вимог, пов'язаних із забезпеченням заходів та засобів захисту, (Всього: 18 год);

$t_{озб}$ - тривалість вибору основних рішень із забезпеченням безпеки інформації, (Всього: 20 год);

$t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування підприємства, (Всього: 18 год);

$t_д$ - тривалість організації на оформлення документованого формату,

(Всього: 3 год).

Як приклад, буде розраховано вартість для політики, пов'язаної із забезпеченням антивірусного захисту в ІТС.

Сумарно витрачений час:

$$t = 14 + 8 + 20 + 18 + 20 + 18 + 3 = 101 \text{ год}$$

3.1.2 Розрахунок витрат на створення політики безпеки інформації для КСЗІ

Підводячи даний термін до рівня комерційних структур можна сказати, що ЕБ в сфері даних компаній це складна багатофакторна категорія, яка підтримує економічний статус підприємства, створює умови конкурентної спроможності між схожими структурами, дає можливість компанії виступати у ролі посередника між населенням і державою задовольняючи потреби обох сторін та певним чином комерційна структура впливає на національну економіку країни.

Необхідно прорахувати, скільки грошових ресурсів втратить компанія на розробку політики безпеки інформації. Визначити можна за даною формулою 3.2:

$$\text{Крп} = \text{Ззп} + \text{Змч} \qquad (3.2)$$

де Крп - витрати на розробку політики;

Ззп - заробітна платня спеціаліста;

Змч - витрачений час на розробку політики.

Для коректного розрахунку премії необхідно розглянути таблицю, де зазначена погодинна платня працівників.

Таблиця 3.1 – Опис погодинної і місячної заробітної платні робітників

№	Посада	Погодинна заробітна платня	Місячна заробітна платня
1	Директор	768,64 грн\год	18 447,36 грн
2	Розробник	384,32 грн\год	9 223,68 грн

3	Тестувальник	276,7 грн\год	6 640,8 грн
4	Бізнес-аналітик	538,05 грн\год	12 913,2 грн
5	Бухгалтер	166,6 грн\год	3 998,4 грн
6	Системний адміністратор	269,02 грн\год	6 456,48 грн
7	Ст. системний адміністратор	538,05 грн\год	12 912,96 грн

Середньо годинна заробітна плата фахівця з інформаційної безпеки, дорівнює 75 грн/год.

Оскільки питаннями ІБ займаються системні адміністратори, то додаткові витрати на премію співробітникам в сфері ІБ складають:

Для системного адміністратора:

$$0.05 \times 269{,}02 \text{ грн} \times 288 \text{ робочих днів} = 3\,873{,}89 \text{ грн}$$

Для старшого системного адміністратора:

$$0.05 \times 538{,}05 \text{ грн} \times 288 \text{ робочих днів} = 7\,747{,}77 \text{ грн}$$

Для знаходження витрат, необхідно прорахувати заробітну платню виконавця наступними формулами 3.3 і 3.4:

$$Ззп = t \times Зіб \quad (3.3)$$

$$Змч = t \times Смч \quad (3.4)$$

де, t - час, витрачений на розробку політики,

Зіб - середня погодинна заробітна платня,

Смч – вартість 1 години машинного часу ПК.

Для визначення часу треба застосувати дані формули 3.5, що описана нижче:

(3.5)

$$\text{Смч} = P * t_{\text{нал}} * C_e + \frac{\Phi_{\text{зал}} * \text{Н}_a}{F_p} + \frac{\text{К}_{\text{лпз}} * \text{Н}_{\text{апз}}}{F_p}, \text{грн.}$$

Р – встановлена потужність;

Се – тариф на електричну енергію;

Фзал – залишкова вартість ПК на поточний рік;

На – річна норма амортизації;

Напз – річна норма амортизації на ліцензійне ПЗ;

Клпз – вартість ліцензійного ПЗ;

Fp – річний фонд робочого часу.

Ліцензійне програмне забезпечення (для одного ПК):

- Windows 10 Pro – 1100 грн;
- Microsoft Office 365 (версія від 2018 року) – 700 грн;
- Microsoft SQL Server (від 2019) - 110грн;
- Microsoft Visual Studio – 1478грн;

(для одного ПК сумарна вартість – 3388 грн);

Кількість ПК: 16

Вартість ліцензійного ПЗ для 16 ПК: 3388 * 16 = 54 208 грн.

Витрати спеціалістам з питань ІБ, що керують і розробляють аудити для співробітників компанії600.00 (1 заняття)

За 1 рік:

4 * 2 = 8 занять\міс

8 * 12 = 96 занять\рік

600.00 * 96 = 57600 грн

Розрахувати ціну можна в залежності від частоти проведення аудитів. Спеціалісти проводять аудити 2 рази на тиждень по 1 годині.

Затрати спеціалістам не амортизуються.

Вартість ПК = 25000 грн, строк корисної служби – 42 місяці.

Накопичена амортизація = $(25000 * 42)/(5 * 12) = 17\ 500$ грн

Залишкова вартість: 25000 - 17500 = 7500 грн.

Можемо сказати, що головним ресурсом реалізації КСЗІ являється грошовий ресурс, але задля того, щоб впроваджувати КСЗІ необхідно проаналізувати економічний рівень безпеки підприємства, з метою встановлення можливості реалізації КСЗІ.

Знаходимо елемент $С_{мч}$ за формулою 3.5:

$$С_{мч} = 0.45 * 2 + \frac{7500*0.4}{1920} + \frac{3388*0.1}{1920} = 2.64 \text{ грн}$$

Виходячи із вищеописаних даних, можемо знайти зарплатню виконавця і витрати машинного часу:

Ззп = 101 * 75 = 7575 грн

Змч = 101 * 2.64= 266.54 грн

Отже, можна розрахувати витрати на розробку політики безпеки. Так як Змч - час, витрачений на розробку політики, можемо зробити розрахунки за формулою 3.2:

Крп = 7575 грн + 266.54 грн= 7 841.54 грн

Повна вартість капітальних витрат розраховуються за формулою 3.6:

$$К = Крп + Каз, \text{ грн.} \quad (3.6)$$

де Крп – вартість розробки КСЗІ, тис. грн.;

Каз – вартість закупівлі апаратного забезпечення та додаткового обладнання, тис. грн.

Для впровадження КСЗІ у закладі необхідно придбати таке апаратне забезпечення:

- Комплекс «Гриф-Мережа» (1 шт. – 7010 грн.; 16 шт. = 7000 * 16 = 112160 грн.)

Таким чином, загальна вартість забезпечення становить:

$$Каз = 112160 \text{ грн}$$

Можемо розрахувати повну вартість капітальних витрат за формулою 3.6:

$$К = 7\ 841.54 \text{ грн} + 112160 \text{ грн} = 120001.54 \text{ грн}$$

3.2. Розрахунок експлуатаційних (поточних) витрат

Наступним етапом розрахунків витрат підприємства буде прорахування поточних витрат на підтримку КСЗІ. Оскільки у даній організації присутні 2 особи, які забезпечують безпеку інформації і адміністрування систем в ІТС і заробітна платня працівників статична (без врахування премій), то витрати на підтримку КСЗІ буде розраховано за нижче описаною формулою 3.7:

$$С = Са + Сз + Се + Се+Сєв+ Слиз, \text{ грн.} \quad (3.7)$$

де Са – річний фонд амортизаційних відрахувань;

Сз – річний фонд заробітної плати інженерно-технічного персоналу;

Се – вартість електроенергії,що споживається апаратурою;

Слиц – річні витрати на оновлення та подовження ліцензій ПЗ.

Річний фонд амортизаційний відрахувань (Са) визначається за формулою 3.8: (3.8)

$$Са = Фп/Т, \text{ грн.}$$

де Фп – первісна вартість придбаного обладнання;

Т – мінімальний термін корисного використання (дорівнює 5 років для апаратного забезпечення).

$$Са = \frac{112160}{5} = 22432 \text{ грн}$$

Річний фонд запробітної плати розраховується за формулою 3.9, для знаходження Сз наступним чином:

$$Сз = Зосн1 + Зосн2 + \dots Зоснn, \quad (3.9)$$

де Зосн - основна заробітна платня робітника інженерно-технічного персоналу.

Сз = 12912.96 + 6456.48 = 19369.44 грн

Витрати на навчання зазначено вище, тобто, Сн = 57600 грн. Вартість електроенергії можна розрахувати за формулою 3.10:

$$Сел = P * Fp * Це, грн, \quad (3.10)$$

де Р - встановлена потужність апаратури ІБ (кВт), Fp - річний фонд робочого часу системи ІБ;

Це - тариф на електроенергію (грн\Квт * год).

Це = 2 грн\кВт*год.

Даний показник встановлений із стандартами договору даного підприємства. За розрахунками даного року встановлена потужність апаратури ІБ складає 4.5 кВт. Аналізуючи режим роботи ІБ(за 40-годинного робочого дня становить 1920)

Отже:

Сел = 2 * 1 * 4.5 * 1920 = 17280 грн

Витрати на технічне і адміністративне керування ІБ визначаються у відсотках від вартості капітальних витрат.

Слиц = 54208грн.

Також, до річного фонду заробітної плати додається єдиний внесок (*Сєв*) на загальнообов'язкове державне соціальне страхування – консолідований страховий внесок.

Розмір єдиного внеску на загальнообов'язкове державне соціальне страхування визначається на підставі встановленого чинним законодавством відсотка від суми основної та додаткової заробітної плати (за узгодженням з керівником економічної частини кваліфікаційної роботи було встановлено 22%):

Сєв = 0.22 * Сз

Сєв = 0.22 *19369.44 = 426.02

Повна вартість річних експлуатаційних витрат:

С = 22432 грн + 19369.44 грн + 17280 грн + 426.02 грн + 54208 грн =

113 715.46 грн

Отже поточні витрати на рік складають 113 715.46 грн враховуючи витрати на підтримку КСЗІ, заробітню платню спеціалістам в сфері ІБ.

3.3. Оцінка величини збитку у разі реалізації загрози

Можна сказати, що так як дана компанія являє собою велику комерційну структуру, то можна надати певні рекомендації стосовно мінімізації витрат на розробку КСЗІ. Головними економічними чинниками даного підприємства будуть:

- Оптова закупівля ресурсів на реалізацію КСЗІ;
- Збільшення продуктивності праці компанії;
- Модернізація або встановлення механізмів захисту фізичного, організаційного або апаратно-технічного характеру без залучення сторонніх комерційних структур, які не входять до складу компанії.

Далі буде прораховано можливі збитки у результаті реалізації загроз. Показники беруться умовні і розрахунки проводяться в межах ІТС підприємства. Доступ до ІТС мають 2 системних адміністратори, 1 бухгалтер, 1 директор, 2 бізнес-аналітика, 5 розробників і 5 тестувальників. Загальна кількість: 16 осіб. Можливі збитки та упущену вигоду можна розрахувати за формулами 3.11-3.13:

$$U = \text{Пп} + \text{Пв} + V \tag{3.11}$$

$$\text{Пп} = \frac{\sum \text{Зс}}{F} \times t\text{п} \tag{3.12}$$

$$\text{Пв} = \text{Пви} + \text{Пвч} + \text{Пзч} \tag{3.13}$$

де, Пп – оплачувані втрати робочого часу;

Пв – вартість відновлення працездатності вузла корпоративної мережі;

Пви – витрати на повторне уведення інформації;

Ппв – витрати на відновлення вузла або сегмента корпоративної мережі;

Пзч – вартість заміни устаткування або запасних частин;

tп – час простою:

F – місячний фонд робочого часу;

V – втрати від зниження обсягу продажів.

Необхідно враховувати погодинну платню співробітників ІТС. Умовно було взято 6 годин простою мережі. Виходячи з цього, можемо прорахувати параметр Пп:

Пп = 768,64 грн\год + 5 розробників × 384,32 грн\год + 2 бізнес-аналітика × 538,06 грн\год + 5 тестувальників × 276,7 грн\год + 269,02 грн\год + 538,05 грн\год + 166,6 грн\год × 6 год = 768,64 грн + 1921,6 грн + 1076,12 грн + 1383,5 грн + 538,05 грн + 166,6 грн × 6 год =35 127,06 грн

Витрати на відновлення інформації і вузла можна знайти за формулами 3.14-3.13:

$$\text{Пви} = \frac{\sum \text{Зви}}{F} \times t\text{ви} \quad (3.14)$$

$$\text{Ппв} = \frac{\sum \text{Зпв}}{F} \times t\text{пв} \quad (3.15)$$

Для того, щоб відновити вузол та втрачені дані співробітникам необхідно по 2 години (умовно) на кожну операцію. Відновлення апаратних частин не буде враховано. Згідно формулам 3.12-3.13:

Пви = Пп = 35 127,06 грн

Ппв = Пви = 35 127,06 грн

Витрати на відновлення вузла будуть залежати від витрат на інженерно-технічний персонал. У нашому випадку, питаннями відновлення вузла корпоративної мережі займаються 2 системних адміністратора, то можемо знайти дані витрати:

Пз = 35 127,06 грн × 2 = 70 254,12 грн

Витрати на зниження обсягу можемо найти за формулою 3.16:

$$V = \frac{O}{Fг \times \text{час відновлення}} \quad (3.16)$$

де Fг – річний фонд робочого часу роботи організації, обсяг продажів атакованого вузла. Умовно було зазначено, що О = 800000 грн\рік.

Підставляючи дані можемо знайти даний елемент:

$$V = \frac{800000 \text{ грн\рік}}{2080 \text{ год} \times 4 \text{ год}} = 2750 \text{ грн}$$

Можемо знайти упущену вигоду за формулою 3.11:

U = 1 340 356.8 грн + 2 680 713.6 грн + 2750 грн = 4 023 820.4 грн

Враховуючи вищеописані збитки, логічним шляхом буде прорахування ефективності систем інформаційної безпеки. Прорахувати дані аспекти можна наступною формулою 3.17:

$$E = B \times R - C \quad (3.17)$$

де В – загальний збиток від атаки;

R – ймовірність реалізації атаки;

С – поточні витрати на підтримку систем інформаційної безпеки.

Знайти загальний збиток атаки необхідно за формулою 3.18:

$$B = \sum i \times \sum n \times U \quad (3.18)$$

де і – ккількість атакованих вузлів;

n – середнє число атак на рік.

За нещодавніми показниками, в ІТС за 2 попередніх роки загалом було атаковано 6 вузлів корпоративної мережі. Можна припустити, що за рік було проведено атаку на 3 вузлів. В середньому за рік було проведено 12 атак.

Отже, можемо прорахувати загальні збитки від атаки:

$$B = 1 \times 12 \text{ атак} \times 70254.12 \text{ грн} = 843049.44 \text{ грн}$$

Ймовірність реалізації загрози умовно було взято як 50%. Можемо прорахувати ефект від впровадження систем інформаційної безпеки.

$$E = 843049.44\text{грн} * 0.5 – 113\ 715.46 \text{ грн} = 307\ 809.26 \text{ грн}$$

Можна сказати, що ефект реалізованої системи інформаційної безпеки достатньо максимально знизить можливі збитки від реалізації атак на вузли та сегменти мережі. Наступним шляхом буде прорахування ефективності систем інформаційної безпеки. По-перше, треба визначити коефіцієнт повернення інвестицій за наступною формулою 3.19:

$$ROSI = \frac{E}{K} \qquad (3.19)$$

де E – загальний ефект від впровадження систем інформаційної безпеки;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект. Отже:

$$ROSI = \frac{307\ 809.26 \text{ грн}}{120\ 001.54 \text{ грн}} = 2.57$$

Останнім пунктом розрахування витрат на реалізацію КСЗІ буде прорахунок терміну окупності, який представляє собою час, необхідний для окупності встановлених систем інформаційної безпеки і впроваджених політики.

Проект системи інформаційної безпеки визнається доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > \frac{(N\text{деп} - N\text{інф})}{100} \qquad (3.20)$$

де *Nдеп* – річна депозитна ставка (20%)

Nінф – річний рівень інфляції (5%)

Оскільки 2.57 > 0.15, проект вважається економічно доцільним.

Термін окупності капітальний інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки, і розраховується за такою формулою 3.21:

$$\text{То} = \frac{E}{K}$$

Порахуємо:

$$\text{То} = \frac{120\,001.54 \text{ грн}}{307\,809.26 \text{ грн}} = 0.39 \approx 4 \text{ місяці.}$$

У останньому підрозділі буде зроблено висновки стосовно даного розділу.

3.4 Висновки до 3 розділу

Підводячи підсумки, можемо сказати, що основною метою даного розділу було обґрунтування економічної доцільності реалізації КСЗІ для ТОВ «Українські Інноваційні Технології», прорахунок всіх витрат на реалізацію КСЗІ в ІТС та надання рекомендацій стосовно зниженню витрат на створення і підтримку КСЗІ.

У підрозділах було розглянуто витрати організації на розробку КСЗІ.

Було проведено такі розрахунки:

- розрахунок капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забеспечення ($K = 307\,809.26$ грн);
- розрахунок річних експлуатаційних витрат на утримання і обслуговування

об'єкта проектування ($C = 113\ 715.46$ грн);

- визначення річного економічного ефекту від впровадження об'єкта проектування (E = 307 809.26 грн);
- отримане значення коефіцієнта ROSI перевищує дохідність альтернативного вкладення коштів, тож рішення є економічно доцільним.
- термін окупності капітальних інвестицій – 4 місяці.

ВИСНОВКИ

Метою кваліфікаційної роботи є захист інформації що обробляється в інформаційно-телекомунікаційній системі на заданому рівні.

У першому розділі було виконано обстеження ІТС, а саме:

- загальна інформація про підприємство;
- персонал та його обов'язки;
- робочі станції підприємства;
- приміщення у якому знаходиться контрольована зона;
- схема мережі підприємства;
- огляд програмного забезпечення підприємства;
- модель порушника;
- актуальні загрози для інформації, що циркулює в ІТС.

У другому розділі було сформульовано вимоги до послуг безпеки інформації у вигляді профілю захищеності. На основі якого запропоновані проектні рішення, що реалізують послуги, які були відсутні.

Для забезпечення захисту інформації були реалізовані наступні рішення:

- нова матриця доступу;
- визначені програми захисту інформації та інструкції до них;
- реалізовані вимоги захищеності інформації за допомогою вбудованих функцій Windows 10 та КЗЗ «Гриф» версії 4 та встановлення допоміжних програм.

У економічному розділі була обґрунтована економічна доцільність реалізації КСЗІ для ТОВ «Українські Інноваційні Технології», прорахунок всіх витрат на реалізацію КСЗІ в ІТС та надання рекомендацій стосовно зниженню витрат на створення і підтримку КСЗІ.

У підрозділах було розглянуто витрати організації на розробку КСЗІ.

Було проведено такі розрахунки:

- розрахунок капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забеспечення;

- розрахунок річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування;
- отримане значення коефіцієнта ROSI перевищує дохідність альтернативного вкладення коштів, тож рішення є економічно доцільним;
- термін окупності капітальних інвестицій – 4 місяці.

ПЕРЕЛІК ПОСИЛАНЬ

1. Відомості Ради національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/ua/Diialnist/4797.html?PRINT

2. Нормативний документ. Технічний захист інформації, термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99. URL: https://tzi.ua/assets/files/1.1_003_99.pdf

3. Нормативний документ. Технічний захист інформації. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.URL:https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf

4. Стаття. Шифрування. URL: https://uk.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F.

5. Стаття. Шифр RSA. URL: https://uk.wikipedia.org/wiki/RSA3.

6. НД ТЗІ 3.7-003-2005 – Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системи. – ДСТСЗІ СБ України, Київ. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf

7. НД ТЗІ 2.5-004-99 – Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу – ДСТСЗІ СБ України – Київ. URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf

8. Експертний висновок КЗЗ «Гриф» версії 4, виробництва ТОВ «Інститут комп'ютерних технологій» №1034 (з 24.10.2019 до 24.10.2022).

9. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 – Кібербезпека. – Національний технічний університет «Дніпровська Політехніка», Факультет інформаційних технологій, кафедра безпеки інформації і телекомунікацій. – Герасіна О.В., Тимофєєв Д.С., Кручінін О.В., Мілінчук Ю.А.

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Таблиця А.1 - Перелік апаратного забезпечення ІТС згідно з рис. 1.

№	**Розміщення**	**Відстань до межі ОІД, м**	**№**	**Розміщення**	**Відстань до межі ОІД, м**
Назва: PC монітор			**Назва:** PC блок		
1	Кімната 1, на столі	1,73	11	Кімната 1, на підлозі	1,73
2	Кімната 2, на столі	0,37	12	Кімната 2, на підлозі	0,37
3	Кімната 2, на столі	0,70	13	Кімната 2, на підлозі	0,70
4	Кімната 4, на столі	0,34	14	Кімната 4, на підлозі	0,34
5	Кімната 4, на столі	2,79	15	Кімната 4, на підлозі	2,91
6	Кімната 5, на столі	2,48	16	Кімната 5, на підлозі	2,78
7	Кімната 5, на столі	0,51	17	Кімната 5, на підлозі	0,51
8	Кімната 5, на столі	0,51	18	Кімната 5, на підлозі	0,51
9	Кімната 3, на столі	1,33	19	Кімната 3, на підлозі	1,33

Продовження таблиці А.1

10	Кімната 3, на столі	1,38	20	Кімната 3, на підлозі	1,38
PC Клавіатура			PC миш		
21	Кімната 1, на столі	1,73	31	Кімната 1, на столі	1,73
22	Кімната 2, на столі	0,37	32	Кімната 2, на столі	0,37
23	Кімната 2, на столі	0,70	33	Кімната 2, на столі	0,70
24	Кімната 4, на столі	0,34	34	Кімната 4, на столі	0,34
25	Кімната 4, на столі	2,39	35	Кімната 4, на столі	2,79
26	Кімната 5, на столі	2,78	36	Кімната 5, на столі	2,78
27	Кімната 5, на столі	0,51	37	Кімната 5, на столі	0,51
28	Кімната 5, на столі	0,51	38	Кімната 5, на столі	0,51
29	Кімната 3, на столі	1,33	39	Кімната 3, на столі	1,33
30	Кімната 3, на столі	1,38	40	Кімната 3, на столі	1,38

Продовження таблиці А.1

Веб-камера						
41	Кімната 1, на столі	1,73	46	Комутатор (К1)	Кімната 3, на столі	0,50
42	Кімната 5, на столі	0,51	47	Сервер(С1)	Кімната 3, на підлозі	0,50
43	Кімната 5, на столі	0,51	48	Маршрутизатор(М1)	Кімната 3, на столі	0,50
44	Кімната 5, на столі	2,98	49	Принтер(ПР1)	Кімната 2, на столі	0,30
45	Кімната 3, на столі	1,20	50	Принтер(ПР2)	Кімната 2, на столі	1,20

Таблиця А.2 - Інвентаризаційна відомість ДТЗС

№	**Назва**	**Марка**	**Модель**	**Серійний номер**	**Розміщення**
1	РСП	SATEL	CA-10 (KLCD-S)	001201	На першому поверсі, біля входу
2	Камера відеоспостереження	KDM	69-19	001202	Кімната 1, на стелі
3	Камера відеоспостереження	KDM	69-19	001203	Кімната 2, на стелі
4	Камера відеоспостереження	KDM	69-19	001204	Кімната 3, на стелі

Продовження таблиці А.2

5	Камера відеоспостереження	KDM	69-19	001205	Кімната 4, на стелі
6	Камера відеоспостереження	KDM	69-19	001206	Кімната 5, на стелі
7	Камера відеоспостереження	KDM	69-19	001207	Коридор, на стелі
8	Камера відеоспостереження	KDM	69-19	001208	Коридор, на стелі
9	Камера відеоспостереження	KDM	69-19	001209	Коридор, на стелі
10	Датчик диму	SimPal	WSD 049-F	001210	Кімната 1, на стелі
11	Датчик диму	SimPal	WSD 049-F	001211	Кімната 2, на стелі
12	Датчик диму	SimPal	WSD 049-F	001212	Кімната 3, на стелі
13	Датчик диму	SimPal	WSD 049-F	001213	Кімната 4, на стелі
14	Датчик диму	SimPal	WSD 049-F	001214	Кімната 5, на стелі
15	Датчик диму	SimPal	WSD 049-F	001215	Коридор, на стелі

Продовження таблиці А.2

16	Датчик диму	SimPal	WSD 049-F	001216	Коридор, на стелі
17	Датчик диму	SimPal	WSD 049-F	001217	Коридор, на стелі
18	Датчик диму	SimPal	WSD 049-F	001218	В туалеті, на стелі
19	Датчик диму	SimPal	WSD 049-F	001219	В туалеті, на стелі
20	Інфрачервоний датчик	Feron	IP-20	001220	Коридор, на стелі
21	Інфрачервоний датчик	Feron	IP-20	001221	Коридор, на стелі
22	Інфрачервоний датчик	Feron	IP-20	001222	Коридор, на стелі
23	Інфрачервоний датчик	Feron	IP-20	001223	Кімната 1, на стелі
24	Інфрачервоний датчик	Feron	IP-20	001224	Кімната 2, на стелі
25	Інфрачервоний датчик	Feron	IP-20	001225	Кімната 3, на стелі
26	Інфрачервоний датчик	Feron	IP-20	001226	Кімната 4, на стелі

Продовження таблиці А.2

27	Інфрачервоний датчик	Feron	IP-20	001227	Кімната 5, на стелі
28	Акустичний сповіщувач	Satel	INDIGO	001228	Коридор, на стелі, на першому поверсі

Таблиця А.3 - Розмежування доступу до техніки матриця доступу

№	Назва	Назва в ІТС	Характеристика	Серійний номер
1	Робоча станція	PC1	Процесор: AMD Athlon II X4 630 4x2.8 GHz 8GT / 12MB / 95Вт/4 Материнська плата: Intel H312 3 x DDR4 DIMM Жорсткий диск: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC (SA400S37/120G) Оперативна пам’ять: HyperX DDR4 - 2666 МГц, 8 ГБ, 32768 МБ	00001
2	Робоча станція	PC2	Процесор: AMD Athlon II X4 630 4x2.8 GHz 8GT / 12MB / 95Вт/4 Материнська плата: Intel H312 3 x DDR4 DIMM Жорсткий диск: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC (SA400S37/120G) Оперативна пам’ять: HyperX DDR4 - 2666 МГц, 8 ГБ, 32768 МБ	00002

Продовження таблиці А.3

3	Робоча станція	PC3	Процесор: AMD Athlon II X4 630 4x2.8 GHz 8GT / 12MB / 95Вт/4 Материнська плата: Intel H312 3 x DDR4 DIMM Жорсткий диск: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC (SA400S37/120G) Оперативна пам'ять: HyperX DDR4 - 2666 МГц, 8 ГБ, 32768 МБ	00003
4	Робоча станція	PC4	Процесор: AMD Athlon II X4 630 4x2.8 GHz 8GT / 12MB / 95Вт/4 Материнська плата: Intel H312 3 x DDR4 DIMM Жорсткий диск: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC (SA400S37/120G) Оперативна пам'ять: HyperX DDR4 - 2666 МГц, 8 ГБ, 32768 МБ	00004
5	Робоча станція	PC5	Процесор: AMD Athlon II X4 630 4x2.8 GHz 8GT / 12MB / 95Вт/4 Материнська плата: Intel H312 3 x DDR4 DIMM Жорсткий диск: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC (SA400S37/120G) Оперативна пам'ять: HyperX DDR4 - 2666 МГц, 8 ГБ, 32768 МБ	00005

Продовження таблиці А.3

6	Робоча станція	PC6	Процесор: AMD Athlon II X4 630 4x2.8 GHz 8GT / 12MB / 95Вт/4 Материнська плата: Intel H312 3 x DDR4 DIMM Жорсткий диск: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC (SA400S37/120G) Оперативна пам'ять: HyperX DDR4 - 2666 МГц, 8 ГБ, 32768 МБ	00006
7	Робоча станція	PC7	Процесор: AMD Athlon II X4 630 4x2.8 GHz 8GT / 12MB / 95Вт/4 Материнська плата: Intel H312 3 x DDR4 DIMM Жорсткий диск: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC (SA400S37/120G) Оперативна пам'ять: HyperX DDR4 - 2666 МГц, 8 ГБ, 32768 МБ	00007
8	Робоча станція	PC8	Процесор: AMD Athlon II X4 630 4x2.8 GHz 8GT / 12MB / 95Вт/4 Материнська плата: Intel H312 3 x DDR4 DIMM Жорсткий диск: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC (SA400S37/120G) Оперативна пам'ять: HyperX DDR4 - 2666 МГц, 8 ГБ, 32768 МБ	00008

Продовження таблиці А.3

9	Робоча станція	PC9	Процесор: AMD Athlon II X4 630 4x2.8 GHz 8GT / 12MB / 95Вт/4 Материнська плата: Intel H312 3 x DDR4 DIMM Жорсткий диск: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC (SA400S37/120G) Оперативна пам’ять: HyperX DDR4 - 2666 МГц, 8 ГБ, 32768 МБ	00009
10	Робоча станція	PC10	Процесор: AMD Athlon II X4 630 4x2.8 GHz 8GT / 12MB / 95Вт/4 Материнська плата: Intel H312 3 x DDR4 DIMM Жорсткий диск: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC (SA400S37/120G) Оперативна пам’ять: HyperX DDR4 - 2666 МГц, 8 ГБ, 32768 МБ	00010
11	Комутатор	K1	Скорость Uplink портов: 1 Гбит Модель: TP-LINK TL-SF1005D Скорость LAN портов: 10/100 Мбит	00011
12	Маршрутизатор	M1	з 3 10/100/1000 Gigabit Ethernet портами, 512 Mb DRAM (max: 2 Gb), 256 Mb Flash (max: 4 Gb), 4 слоти EHWIC, 2 DSP, 1 ISM, AC блок живлення	00012

Продовження таблиці А.3

13	Сервер	С1	Процесор: восьмиядерна Intel Xeon Q-1098G (3.7 - 5.0 ГГц), Об'єм оперативної пам'яті: 128 ГБ, HDD: 2 x 4 ТБ SSD: 2 x 1 ТБ Samsung, Швидкість LAN: Gigabit Ethernet	00013
14	Принтер	ПР1	Лазерний друк (кол), 1800x900 dpi, 12 стр / хв (А4)	00014
15	Принтер	ПР2	Лазерний друк (ч / б), 1800x900 dpi, 12 стр / хв (А4)	00015
16	Веб-камера	В1	1600x900, з мікрофоном, прищіPCa, USB 2.0, 30 частота кадрів в секунду	00016
17	Веб-камера	В2	1600x900, з мікрофоном, прищіPCa, USB 2.0, 30 частота кадрів в секунду	00017
18	Веб-камера	В3	1600x900, з мікрофоном, прищіPCa, USB 2.0, 30 частота кадрів в секунду	00018
19	Веб-камера	В4	1600x900, з мікрофоном, прищіPCa, USB 2.0, 30 частота кадрів в секунду	00019

Таблиця А.4. - Інвентаризаційна відомість програмного забезпечення ІТС

№	**Назва**	**Опис**	**Ліцензія**	**Де встановлена**
Тип: Системне				
1	Windows 10 10.0.18004.2 (build 1809)	Операційна система для персональних комп'ютерів і робочих станцій	Volume license	PC1 – PC10
2	Windows Server 2019	Операційна система для серверів	Volume license	C1

Продовження таблиці А.4

3	ESET File Security (версія 7.1.12008)	Антивірусна програма	Commercial	PC1 – PC10
4	WinRar (версія 5.8)	Архіватор файлів для 32- і 64-розрядних операційних систем Windows	Shareware	PC1 – PC10
Прикладне				
5	Базовий пакет Microsoft Office 2019 Professional	ПЗ для роботи з різними видами документів, текстів, таблиць, базами даних тощо.	Volume license	PC1 – PC10
6	1С Підприємство 8.3. Базова версія	Програми, що дозволяють виконувати операції над даними, представленими в табличній формі	Volume license	PC1 – PC10
7	Adobe Photoshop CS6 (версія 13.05)	Засоби створення нерухомих і рухомих зображень	Volume license	PC10
8	Microsoft Edge (версія 44.18364.0.0)	Програми для роботи в комп'ютерній мережі	Freeware	PC1 – PC10
9	Google Chrome (версія	Програми для роботи в комп'ютерній мережі	Freeware	PC1 – PC10

	80.0.3987)			

Продовження таблиці А.4

10	Windows Media Player (версія 12.0.18362.418)	Програма для відтворення відео- та аудіофайлів	Freeware	PC1 – PC10
		Спеціальне		
11	Visual Studio 2019 (версія 16.0)	Об'єктно-орієнтовані мови програмування	Volume license	PC9, PC10
12	TeamViewer (версія 15.4.4445)	Програми для роботи в комп'ютерній мережі через віддалений доступ	Freeware	PC1 – PC10
13	Adobe Acrobat (версія 2019.008.20071)	Програма для роботи з pdf-файлами	Freeware	PC1 – PC10
14	Skype (версія 14.56.102.0)	Програма забезпечує текстову, голосовий та відеозв'язок через Інтернет між комп'ютерами	Freeware	PC1 – PC10
15	Viber (версія 12.6.0.41)	Програма забезпечує текстову, голосовий та відеозв'язок через Інтернет між комп'ютерами	Freeware	PC1 – PC10

ДОДАТОК Б. ФОРМА ТА ЗМІСТ АКТУ КАТЕГОРІЮВАННЯ ОБЄКТУ

ЗАТВЕРДЖУЮ
Керівник установи-власника
(розпорядника, користувача) об'єкта
ректор Кришталь М.П.
(посада, підпис, ініціали, прізвище)
20.05. 2022

АКТ
категоріювання інформації інформаційно-телекомунікаційної системи ТОВ «Українські Інноваційні Технології»
(найменування об'єкта категоріювання)

1. Підстава для категоріювання рішення про створення КСЗІ
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
зміна ознаки, за якою була встановлена категорія об'єкта, тощо;
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання: первинне
(первинне, чергове, позачергове)
(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється обробка інформації технічними засобами
(обробка інформації технічними засобами та/або озвучування інформації)

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті: конфіденційна інформація
(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації"; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія: 4 категорія

Голова комісії _____ Коваленко Р. О.
(підпис) (ініціали, прізвище)
Члени комісії: _____ Корнілєнко М.М.
(підпис) (ініціали, прізвище)

20.05.2022

ДОДАТОК В. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

1. Удовик_МО_125_18_1_ПЗ.docx
2. Удовик_МО_125_18_1_ПЗ.pdf
3. Удовик_МО_125_18_1_ПЗ.pdf.p7s
4. Удовик_МО_125_18_1_ДМ.pptx

ДОДАТОК Г. ВІГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

В І Д Г У К

на кваліфікаційну роботу студентки групи 125-18-1

Удовик Марії Олексіївни

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «Українські Інноваційні Технології»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 95 сторінках.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІТС ТОВ «Українські Інноваційні Технології».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: обстеження середовищ функціонування ІТС, розробка моделі порушника, визначення актуальних загроз, формування вимог до захисту інформації та розробка проектних рішень їх реалізації.

Запропоновано матрицю розмежування доступу, розроблені положення політики безпеки щодо паролів. Запропоновані налаштування журналу подій та систем самотестування. Розроблені проектні рішення впровадження додаткового КЗЗ та захищеного з'єднання через незахищені канали зв'язку.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих рішень до особливостей ТОВ «Українські Інноваційні Технології».

До недоліків відноситься недостатньо обґрунтована модель загроз та реалізації окремих послуг безпеки.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Удовик М.О. проявила себе фахівцем, здатним достатньо самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «добре».

Керівник кваліфікаційної роботи, професор Корнієнко В.І.

Керівник спец. розділу, ст. викладач Кручінін О.В.

ДОДАТОК Ґ . ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОЇ ЧАСТИНИ

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)